DINÁMICA DEL RIESGO OPERATIVO EN EL SECTOR FINANCIERO CON UN ENFOQUE SISTÉMICO A PARTIR DE LA SIMULACIÓN DE EVENTOS DE RIESGO

LAURA ARBOLEDA GUTIÉRREZ
MARÍA FERNANDA BRAVO LÓPEZ

Trabajo de grado para optar al título de ingeniero administrador

Jaime Alberto Sánchez Velásquez

MSc Ingeniería- Ingeniería Administrativa

UNIVERSIDAD EIA
INGENIERÍA ADMINISTRATIVA
ENVIGADO
2018

AGRADECIMIENTOS

Gracias universidad EIA, gracias por habernos permitido formarnos y en ella, gracias a todas las personas que fueron participes de este proceso, ya sea de manera directa o indirecta, gracias a todos ustedes , fueron responsables de realizar su pequeño aporte que el día de hoy se vería reflejado en la culminación de nuestro paso por la universidad. Queremos agradecer principalmente al profesor Jaime Alberto Sánchez, director de este trabajo de grado, quien creyó en este proyecto, nos apoyó de manera personal e institucional y nos alentó para concluir satisfactoriamente esta investigación.

De igual forma queremos agradecer a nuestros padres, quienes fueron nuestro mayor soporte en este proceso y quienes siempre confiaron y creyeron en nuestros sueños. Gracias por siempre brindarnos lo mejor y buscar nuestro bienestar a pesar de las adversidades. Gracias a nuestras familias y amigos por apoyarnos en este grandísimo reto llamado universidad, y por siempre estar ahí.

El camino hasta este momento no ha sido sencillo, pero agradecemos sus aportes, apoyo, enseñanzas y amor que nos han transmitido. Cada momento vivido durante todos estos años, son simplemente únicos y por eso damos gracias a la vida por este nuevo triunfo.

CONTENIDO

pág.

LISTA DE TABLAS

pág.

LISTA DE FIGURAS

pág.

LISTA DE ANEXOS

pág.

GLOSARIO

RIESGO OPERACIONAL: posibilidad de incurrir en pérdidas por deficiencias, fallas o inadecuaciones, en el recurso humano, los procesos, la tecnología, la infraestructura o por la ocurrencia de acontecimientos externos.

SECTOR FINANCIERO: sector conformado por las instituciones financieras y sus fondos administrados y regulados en Colombia por la Superintendencia Financiera.

COMITÉ DE SUPERVISIÓN BANCARIA DE BASILEA: principal órgano normativo internacional para la regulación bancaria. Su objetivo es mejorar la regulación, la supervisión y las prácticas bancarias en todo el mundo con el fin de afianzar la estabilidad financiera

EVENTOS DE RIESGO: posibilidad de pérdidas causadas por variaciones de los factores que afectan el valor de un activo.

FRECUENCIA DE LA PÉRDIDA: cantidad de veces que se repite un evento de pérdida.

SEVERIDAD DE LA PÉRDIDA: costo de reparar el daño generado por el evento de pérdida.

CAPITAL REGULATORIO: recursos con los que debe contar una entidad financiera para poder absorber las posibles pérdidas a las que puede enfrentarse debido a los eventos de riesgo

GESTIÓN DEL RIESGO OPERATIVO: garantizar la identificación y administración eficiente de los riesgos operacionales de forma rentable al reconocer los niveles de riesgo operacional que pueden afectar a la entidad financiera según su apetito de riesgo.

MODELO DINÁMICO: sistema cuyo estado evoluciona con el tiempo ya que algunos elementos que intervienen en la modelización se consideran como funciones del tiempo, describiendo trayectorias temporales

DINÁMICA DE SISTEMAS: metodología mediante la cual es posible crear modelos de sistemas con cierto grado de complejidad donde las variables interactúan en forma constante con el medio. El comportamiento del sistema se puede mostrar a través de diagramas causales.

RELACIONES DINÁMICAS: interacción entre las variables exógenas y endógenas que afectan a un sistema.

MÁXIMO VALOR EN RIESGO OPERACIONAL (OpVaR): máxima pérdida esperada dado un nivel de confianza (α) en un período de tiempo.

RESUMEN

La globalización y desregulación de los servicios financieros han ocasionado que las actividades de los bancos sean cada vez más diversas y complejas, generando a su vez perfiles de riesgo que requieren de métodos de medición y control más sofisticados y adaptados a las realidades de las instituciones; y además que permitan cumplir con los requerimientos propuestos por el Comité de Supervisión Bancaria de Basilea. Particularmente, el riesgo operativo ha cobrado una relevancia importante dentro del sector debido al aumento de pérdidas monetarias por fallos en los sistemas tecnológicos, en el comercio electrónico o factores externos, incrementando así el impacto social del riesgo operativo. Sin embargo, los métodos actuales para la gestión del riesgo operativo no permiten obtener resultados uniformes para entidades con iguales perfiles de riesgo, por tanto, se pretende estudiar cómo el enfoque sistémico puede aportar a la generación de un método estándar para la gestión del riesgo operativo en las entidades financieras, y si este enfoque genera soluciones más robustas al considerar el riesgo operativo sistémicamente.

Para dar solución al problema planteado, el marco metodológico estará basado en la Teoría del Iceberg de Daniel Kim, con especial énfasis en los niveles de eventos, patrones y estructuras. Teniendo como base esta teoría se establecieron cuatro etapas: simulación de datos de eventos de riesgo, utilización del enfoque de distribución de pérdidas (LDA), aplicación de la Teoría General de Sistemas y planteamiento del modelo final. El modelo dinámico planteado se centró en el riesgo de seguridad en los sistemas, a partir de este se capturaron los datos de frecuencia y severidad del evento de riesgo y se calculó el OpVar por medio de 100 simulaciones del modelo de 12 meses. Posteriormente se evaluó el impacto de las decisiones de gestión en el cálculo del OpVar. Con la metodología propuesta se planteó un modelo de gestión y cuantificación de riesgo operativo con un enfoque sistémico que puede ser generalizado en cualquier entidad financiera.

Palabras claves: riesgo operacional, gestión del riesgo, dinámica de sistemas, sector financiero, modelo dinámico, estructuras, enfoque sistémico.

ABSTRACT

The globalization and deregulation of financial services have caused the activities of banks to be increasingly diverse and complex, generating at the same time risk profiles that require more sophisticated measurement and control methods adapted to the realities of the institutions. Also, that they compliance with the requirements proposed by the Basel Committee on Banking Supervision. Particularly, operational risk has gained significant importance within the sector due to the increase in monetary losses due to failures in technological systems, in electronic commerce or external factors, thus increasing the social impact of operational risk. However, current methods for managing operational risk do not allow to obtain uniform results for entities with equal risk profiles, therefore, it is intended to study how the systemic approach can contribute to the generation of a standard method for operational risk management in financial institutions, and if this approach generates more robust solutions when considering operational risk systemically.

To solve the problem, the methodological framework was based on Daniel Kim's Icerberg Theory, with special emphasis on the levels of events, patterns and structures. Based on this theory, four stages were established: simulation of risk event data, use of the loss distribution approach (LDA), application of the General Systems Theory and approach of the final model. The dynamic model proposed focus on the security risk in the systems, the frequency and severity data of the risk event were captured from it, and the OpVar was calculated by 100 simulations of the model for 12 months. Subsequently, the impact of management decisions on the calculation of OpVar was evaluated. With the proposed methodology, a management and quantification model of operational risk was proposed with a systemic approach that can be generalized in any financial institution.

Keywords: operational risk, risk management, system dynamics, financial sector, dynamic model, structures, systemic approach.

INTRODUCCIÓN

El estudio del riesgo operativo en el sector financiero como una práctica integral es relativamente nuevo comparado con el riesgo crédito o de mercado, sin embargo, factores como el crecimiento de los mercados, la diversificación de productos y servicios financieros, además del aumento de casos en todo el mundo de pérdidas por riesgo operativo, han llevado a los bancos y supervisores a considerar la gestión del riesgo operativo como una disciplina integral dentro del sector (Comité de Supervisión Bancaria de Basilea, 2003).

Este tipo de riesgo puede definirse como "la posibilidad de incurrir en pérdidas por deficiencias, fallas o inadecuaciones, en el recurso humano, los procesos, la tecnología, la infraestructura o por la ocurrencia de acontecimientos externos" (Superintendencia Financiera de Colombia, 2006). Teniendo en cuenta esta definición, la industria bancaria ha identificado que grandes instituciones financieras a nivel mundial han experimentado más de 100 eventos de pérdidas operacionales, cada uno de más de $100 millones de dólares en la última década (Galloppo & Rogora, 2011). El Comité de Basilea ha realizado igualmente varias investigaciones para estudiar la severidad del riesgo operativo, en una de ellas investigó 89 bancos con datos de un año lo cual dejó en evidencia 4700 eventos de pérdidas relacionados con el riesgo operacional, que en total sumaron 7.8 billones de euros de pérdidas. Así, la severidad de los eventos operacionales de las instituciones financieras ha hecho evidente la necesidad de generar un sistema eficaz de gestión y medición del riesgo operativo. (Galloppo & Rogora, 2011)

Los bancos han constatado que los problemas operacionales, lo cuales han sido observados durante más de 15 años, pueden resultar más peligrosos que los riesgos financieros (López Pacheco, 2009), por esto las organizaciones buscan mitigar el riesgo reduciendo la vulnerabilidad mediante controles ajustables en eventos individuales de pérdidas, y considerando aspectos de seguridad y control (Kessler, 2007). En Colombia, la Superintendencia Financiera (2007) establece que todas las entidades que estén bajo su vigilancia y regulación deben desarrollar, establecer, implementar y mantener un Sistema de Administración de Riesgo Operativo (SARO). El SARO es un sistema que consiste en un conjunto de elementos tales como políticas, procedimientos, documentación, estructura organizacional, registro de eventos de riesgo operativo, órganos de control, plataforma tecnológica, divulgación de información y capacitación; mediante los cuales las entidades vigiladas identifican, miden, controlan y monitorean el riesgo operativo. (Compañía Aseguradora de Finanzas S.A, 2011).

A pesar de la existencia de los sistemas de administración de riesgo como el mencionado anteriormente, los métodos disponibles para cuantificarlo no otorgan resultados únicos o estandarizados para entidades con perfiles similares, además otorgan resultados únicamente a nivel de predicciones con el fin de generar patrones que faciliten un mayor control del riesgo (Kessler, 2007). El enfoque de la Distribución de Pérdidas, el cual es el más utilizado por el sector, calcula el capital regulatorio como el percentil 99.9% de la

distribución de pérdidas del año siguiente, obteniendo el Valor de Riesgo Operativo (OpVar), este se interpreta como la máxima pérdida esperada dado un nivel de confianza (α) en un período de tiempo (Moosa, 2007). Sin embargo, este enfoque genera un amplio rango de resultados dependiendo de la forma como la institución lo aplique, lo cual pone en manifiesto que la medición del riesgo operacional sigue abierta, y que dejar a elección de los bancos la metodología podría llevar a una significativa infravaloración o sobrevaloración del capital económico operacional (Di Pietro, Irimia-Diéguez, & Oliver-Alfonso, 2012).

Según la Teoría del Iceberg de Daniel Kim (1996), el nivel de patrones es tan solo el segundo de los cuatro niveles de conocimiento existentes en el mundo: eventos, patrones, estructuras y modelos mentales. Los patrones permiten observar los cambios de las variables en el tiempo y, por tanto, especular sobre la posible relación entre eventos, cuando se llega a este nivel es posible anticipar, planear y pronosticar para reaccionar efectivamente ante los problemas. El enfoque analítico para el riesgo operativo permite a las entidades financieras lo expresado anteriormente, anticiparse para ejecutar una respuesta rápida, efectiva y eficiente ante un evento de riesgo; no obstante, estos modelos no responden a la pregunta ¿qué está causando el patrón que se está observando? Para dar respuesta al interrogante planteado, se debe estudiar el nivel de estructuras, ya que estas son las que soportan y crean los patrones observables en los eventos, pues están compuestas de relaciones causa-efecto, las cuales son las conexiones entre patrones (Huigens, 2005). El enfoque sistémico al medir y delimitar cómo el capital, las personas y la información fluyen dentro y fuera de la organización, enfatizando en las interacciones y conexiones entre los diferentes componentes del sistema, puede aportar a la generación de un modelo estándar para la cuantificación y gestión del riesgo operacional que otorgue un resultado superior en la mitigación de la severidad de los eventos de pérdidas (Kessler, 2007).

Así, teniendo en cuenta lo anterior, en el presente trabajo se planteará un modelo de gestión del riesgo operativo generalizado, para el sector financiero, a partir de la simulación de datos de pérdida de eventos de riesgo con un enfoque sistémico. Inicialmente se identificará el patrón de comportamiento del riesgo operativo de los datos simulados para así establecer la estructura causal que genera el patrón de comportamiento de riesgo operativo y por último poder desarrollar escenarios mediante la simulación de la estructura causal a partir de la dinámica de sistemas.

1. PRELIMINARES

1.1 PLANTEAMIENTO DEL PROBLEMA

El sector financiero posee una importancia relevante dentro de la estabilidad económica de un país, esto fue constatado durante la crisis de 2008 donde la poca regulación y fortaleza del sector, originaron el colapso financiero en las principales potencias económicas del mundo; y es a partir de lo anterior que este sector comienza a ser estrictamente regulado tanto por instituciones locales e internacionales con el fin de asegurar su correcto funcionamiento (Aguirre Botero & Mesa Callejas, 2009). En Colombia, la Superintendencia Financiera siguiendo los lineamientos del Comité de Basilea, entidad encargada de la supervisión bancaria a nivel mundial, establece las normativas que deberán adoptar las empresas del sector en su funcionamiento, y en especial en su gestión de los riesgos. (Hernández Correa, 2016)

Los esfuerzos de regulación en los últimos años de las diferentes entidades tanto a nivel local como internacional, además de ser consecuencia de un hito económico importante como lo fue la crisis financiera del 2008, también surgen debido a la creciente desregulación, globalización de los servicios financieros y sofisticación de la tecnología del sector. Lo anterior ha ocasionado que las actividades de los bancos sean cada vez más diversas y complejas, y, por tanto, también sus perfiles de riesgo (Jiménez Rodríguez & Matín Marín, 2005). De esta forma, a pesar de que el riesgo operacional siempre ha existido como uno de los riesgos inherentes a la industria, el aumento del comercio electrónico o el uso de tecnologías altamente automatizadas ha llevado a las entidades bancarias, y a sus reguladores a reconocer la importancia del riesgo operacional en la configuración del perfil de riesgo de las entidades. (Galloppo & Rogora, 2011)

Por mucho tiempo el enfoque analítico ha sido el principal enfoque en la gestión del riesgo operativo, pero el problema de este enfoque es que reduce los eventos de riesgo que suelen ser complejos en partes, lo que resulta en la pérdida de propiedades importantes a la hora de plantear un marco de gestión efectivo (Kessler, 2007). Además, la flexibilidad que permite el Comité de Basilea a la hora de implementar los diferentes enfoques de medición avanzada (AMA) para el riesgo operacional, ha generado en la práctica una diversidad de modelos personalizados con resultados diferentes. Lo anterior quiere decir que bancos con iguales perfiles de riesgo operacional obtienen diferentes niveles de capital regulatorio, generando una estimación a la baja o sobreestimación de este. (Di Pietro, Irimia-Diéguez, & Oliver-Alfonso, 2012)

Teniendo en cuenta lo anterior se pretende estudiar cómo el enfoque sistémico puede aportar a la generación de un método estándar para la gestión del riesgo operativo en las entidades financieras, y si este enfoque genera soluciones más robustas al considerar el riesgo operativo sistémicamente.

1.2 OBJETIVOS DEL PROYECTO

1.2.1 Objetivo General

Plantear un modelo de gestión del riesgo operativo generalizado, para el sector financiero, a partir de la simulación de datos de pérdida de eventos de riesgo con un enfoque sistémico.

1.2.2 Objetivos Específicos

- Identificar el patrón de comportamiento del riesgo operativo de los datos simulados.
- Establecer la estructura causal que genera el patrón de comportamiento de riesgo operativo.
- Desarrollar escenarios mediante la simulación de la estructura causal con dinámica de sistemas.

1.3 MARCO DE REFERENCIA

1.3.1 Antecedentes

La magnitud de las pérdidas operativas observadas en los últimos años, y sus posibles efectos sistémicos, han planteado la necesidad de desarrollar modelos cuantitativos de gestión de riesgo más reales y sofisticados (Brechmann, Czado, & Paterlini, 2013). Así, teniendo en cuenta lo anterior, Brechmann, Czado, & Paterlini (2013) presentaron un enfoque de modelado multivariado bastante flexible para determinar las pérdidas ocasionadas por el riesgo operativo, tomando en cuenta la dependencia multivariada entre las pérdidas, y que los datos de riesgo operacional generalmente son escasos. En el modelo de dependencia "Inflado-Cero", estos autores consideraron familias flexibles de distribuciones para modelar a profundidad la dependencia bivariada entre las pérdidas, y así estimar el capital total de riesgo para las distribuciones de siete tipos de riesgo y ocho líneas de negocio comerciales al usar datos reales. A partir de los resultados empíricos del modelo, Brechmann et al. (2013) concluyeron que las distribuciones de Gauss y t-Student pueden proporcionar un buen ajuste a las pérdidas positivas agrupadas por tipo de riesgo y línea de negocio, esto a pesar de que Gauss implica dependencia de la cola cero y que la distribución t-Student produce una sobreestimación potencial de la dependencia de la cola debido a su inflexibilidad respecto a los grados de libertad.

Desde otra perspectiva, Kessler (2007) en su tesis doctoral propone que la gestión del riesgo operativo puede entenderse como un concepto basado en sistemas, lo que quiere decir que gran parte de los errores operativos de las organizaciones pueden evitarse mediante el diseño correcto del mismo. De esta forma la autora propone un marco de enfoque sistémico para el riesgo operacional que considera aspectos técnicos y no técnicos para combinarlos en la formación de un sistema coherente. En el desarrollo de la propuesta se realiza un caso de estudio con la aplicación en un banco, en este se encuentra que si

los procesos de flujo de trabajo están bien definidos para cada línea de productos de la entidad, este tipo de riesgo puede ser indudablemente definido y modelado. Finalmente, el estudio concluye que el enfoque planteado es relevante para la implementación de un marco avanzado de la gestión del riesgo operativo, puesto que reduce significativamente los costos de medición del riesgo, permite tener un mayor control sobre las pérdidas con baja frecuencia y alta severidad, y permite detectar los eventos de riesgo con mayor anticipación.

En un tercer estudio presentado por Li, Yi et al. (2011) se buscaba reconocer la mitigación de algunos riesgos asociados con el seguro como el incumplimiento de la contraparte, la incertidumbre de pago y la demora de pago, en la modelación de los riesgos operacionales. Esta investigación fue desarrollada teniendo en cuenta que en el año 1999 el Comité de Supervisión Bancaria de Basilea, debido a las enormes pérdidas operacionales de ciertas entidades financieras en el año 1995, estableció que estas entidades debían establecer un capital regulatorio para soportar las pérdidas ocasionadas por diferentes riesgos, entre los cuales está el operacional. Por lo anterior, los autores modelaron el incumplimiento de la contraparte y la incertidumbre de pago bajo el enfoque de la distribución de pérdidas (LDA) con el fin de cuantificar el capital regulatorio para bancos comerciales, teniendo en cuenta que para ellos el método de modelado es favorable ya que permite determinar con éxito el valor predeterminado de la contraparte y qué pérdida no es posible recuperar. Esta investigación permitió que Li, Yi et al. (2011) descubrieran que el factor de incumplimiento de la contraparte no tiene impactos significativos en la mitigación del riesgo, y por ende en el cálculo del capital regulatorio, esto especialmente cuando la aseguradora tiene una calificación crediticia aceptable. Sin embargo, se menciona que no se puede ignorar en la gestión del riesgo operacional porque podría ocasionar una gran pérdida de responsabilidad en un año específico.

Adicionalmente la complejidad de las relaciones existentes entre las empresas que conforman una cadena de suministro ha aumentado considerablemente en las últimas décadas, lo cual motivó a Guertler & Spinler (2015) a realizar un estudio con el fin de determinar en qué momento el riesgo operacional ocasiona que las empresas de la cadena de suministro colapsen. Para esta investigación, ambos autores inicialmente revisaron la literatura existente donde encontraron que las organizaciones deben evaluar las empresas que conforman sus cadenas de suministro en términos de competitividad de precios, fallas potenciales en los productos y el riesgo operacional. No obstante, descubrieron que este último aspecto rara vez es tenido en cuenta al momento de tomar decisiones, por lo cual decidieron estudiar la interrelación existente entre los diferentes riesgos operacionales que se pueden presentar dentro de una empresa de la cadena de suministro. De esta manera, los autores construyeron un modelo de dinámica de sistemas intra-organizacional para analizar el comportamiento de los diferentes riesgos dentro de la organización, además de utilizar la simulación Monte Carlo con la intención de determinar la probabilidad de ocurrencia de un riesgo operacional. Así, a partir de este estudio se pudo demostrar, gracias a un análisis de escenarios, que un riesgo operacional altamente interrelacionado puede afectar en mayor medida a una empresa en comparación a un riesgo débilmente interrelacionado; por lo cual fue válido concluir que un modelo de dinámica de sistemas permite capturar y analizar de forma eficiente las dinámicas internas de una organización (Guertler & Spinler, 2015).

Desde otra perspectiva también se ha estudiado el efecto del riesgo operacional en otro tipo de riesgos que puede aumentar el impacto económico de los eventos de pérdida. Por ejemplo, en el estudio presentado por Christian Eckert y Nadine Gatzert (2016) en la Friedrich–Alexander University Erlangen-Nürnberg (FAU) de Alemania, se realizó un análisis integrado para las empresas financieras al modelar el riesgo operacional teniendo en cuenta las pérdidas reputacionales. Esta investigación fue planteada de esta manera debido a que el riesgo de pérdida de reputación es uno de los riesgos más relevantes para las empresas, y además el riesgo más difícil de medir dentro de cualquier categoría específica de riesgo. Por lo anterior, los autores integraron las pérdidas reputacionales ocasionadas por las pérdidas operacionales, en un modelo existente de riesgo operativo; donde también se consideraron las consecuencias financieras de una reputación dañada al momento de evaluar los tipos de riesgo operacional. Este estudio permitió concluir que los eventos de fraude interno y externo son los más relevantes en términos de pérdidas totales de una compañía; además, estos autores identificaron que la diversificación entre los distintos tipos de eventos de riesgo es relevante para el riesgo operacional y reputacional, puesto que esta diversificación puede reducir considerablemente el riesgo global dependiendo de los factores considerados. Así, este modelo sugiere que la gestión de riesgos debe hacer énfasis en implementar medidas para reducir la probabilidad de ocurrencia e impacto de estos eventos.

Finalmente, en la literatura se encuentran estudios que relacionan directamente la dinámica de sistemas y el sector financiero que es el foco de interés de esta investigación. Santini et al. (2012) presentan en un estudio cómo los riesgos relacionados al comportamiento operacional del sector tecnológico pueden ser simulados, y como a partir de esta simulación se pueden obtener las pérdidas esperadas y el valor en riesgo operacional (OpVar); además utilizan la configuración dinámica para minimizar los riesgos operacionales modelados. Para lograr su objetivo los autores utilizaron técnicas de simulación híbrida obteniendo datos simulados que permiten proyectar a futuro en lugar de analizar eventos pasados, lo cual otorga la posibilidad de estimar los parámetros de las distribuciones teóricas obtenidas. Los resultados de este estudio sirven como base para aumentar la efectividad y eficiencia de las prácticas actuales en la medición del riesgo operativo, sin embargo, debe verificarse si el enfoque propuesto satisface los criterios de los métodos de medición avanzada y las necesidades diarias de los bancos.

Nazareth y Choi (2014) hacen uso del modelado de dinámica de sistemas para evaluar estrategias alternativas para la administración de los sistemas de seguridad mediante la perspectiva de costos e inversión con el fin de proveer a los administradores una guía para las decisiones entorno a los sistemas de seguridad. El modelo creado incorpora diferentes aspectos de la práctica de seguridad incluyendo ataques, detección, recuperación, evaluación de riesgos y disminución de la vulnerabilidad. Los resultados obtenidos sugieren que invertir en herramientas de detección de seguridad tiene una mayor rentabilidad que la inversión de disuasión, además las simulaciones realizadas indican que invertir en todas las áreas de seguridad es necesario para proteger los activos de información. No obstante, el mayor aporte de este estudio es servir con una herramienta para otros investigadores a la hora de tomar decisiones respecto a la seguridad de la información en las instituciones bancarias.

Dada la información anterior, puede constatarse que el riesgo operacional ha sido ampliamente estudiado en la literatura debido a su relevancia económica y de impacto social en las organizaciones. Asimismo, se observa como existen distintos enfoques desde los cuales puede abordarse este riesgo para la formulación de modelos y técnicas que permitan su gestión, siendo la perspectiva sistémica uno de ellos.

1.3.2 Marco teórico

El sector financiero colombiano está conformado por las instituciones financieras y sus fondos administrados. Bajo la vigilancia de la Superintendencia Financiera se encuentran los establecimientos de crédito (EC); las sociedades de servicios financieros (SSF) y otras instituciones financieras, las cuales, en su mayoría, se han agrupado mediante la figura de los conglomerados financieros, haciendo presencia tanto en el ámbito nacional como internacional. Luego de la crisis financiera de finales de la década de los noventa, este sector se ha venido fortaleciendo gracias a la regulación del gobierno nacional y de la Superintendencia Financiera de Colombia (SFC), lo que se ha reflejado en buenos indicadores de rentabilidad, riesgo y solvencia. (Banco de la República, 2013)

Según Coltefinanciera (2017), la principal función de los establecimientos de crédito consiste en captar en moneda legal recursos del público, ya sea en depósitos a la vista (cuentas de ahorro, corriente) o a término (CDT y CDAT´S), para colocarlos nuevamente a través de préstamos, descuentos, anticipos u otras operaciones activas de crédito. Para Coltefinanciera (2017) son establecimientos de crédito:

- **Establecimientos Bancarios**: se centran en la captación de recursos en cuenta corriente bancaria y de otros depósitos a la vista o a término, con el objetivo básico de realizar operaciones activas de crédito.
- **Corporaciones Financieras**: tienen por objeto la movilización de recursos y la asignación de capital para promover la creación, reorganización, fusión, transformación y expansión de cualquier tipo de empresas, así como para participar en su capital, promover la participación de terceros, otorgarles financiación y ofrecer servicios financieros que contribuyan a su desarrollo.
- **Compañías de Financiamiento**: su función principal es la de captar recursos del público con el propósito de financiar la comercialización de bienes y servicios, además de realizar operaciones de arrendamiento financiero o leasing.
- **Cooperativas Financieras**: realizan actividades financieras en los términos de la ley que los regula.

En cuanto a las sociedades de servicios financieros, el Banco de la República (2013) plantea que estas son consideradas instituciones financieras pues, aunque no son intermediarios de recursos financieros, tienen como función principal prestar asesoría financiera especializada en la administración de recursos, por lo cual se consideran como instituciones que prestan servicios complementarios y conexos con la actividad financiera. Los riesgos que se generan en la actividad de las SSF son diferentes de los que se originan en la labor de intermediación de los EC, ya que en las primeras su labor es de medio y no de resultado. Así, según el Banco de la República, riesgos como el operacional, el legal y

el de reputación se hacen críticos en la segunda clase de entidades, ya que la mayoría se orienta a administrar recursos. Algunas de las SSF más relevantes para el Banco de la República (2013) son:

- **Almacenes Generales de Depósito**: custodian mercancías sobre las que se expiden certificados de depósito, los cuales son títulos valores negociables.
- **Sociedades Administradoras de Inversión (SAI)**: se encargan de captar capital del sector privado con el fin de administrarlo y gestionarlo mediante fondos de inversión colectiva y fondos de capital privado.
- **Sociedades de Intermediación Bancaria y de Servicios Financieros Especiales**: realizan operaciones de cambio y efectúan pagos, recaudos, giros y transferencias nacionales en moneda nacional. Estas son corresponsales no bancarios y antes eran conocidas como casas de cambio.

Además de las entidades anteriormente mencionadas, para el Banco de la República (2013) las SSF se conforman por las Sociedades Fiduciarias, Sociedades Administradoras de Pensiones y Cesantías, Sociedades de Capitalización y Sociedades Comisionistas de Bolsa. Las instituciones financieras restantes fueron agrupadas en conglomerados, pues con las modificaciones que se le realizaron al Código de Comercio mediante la Ley 222 de 1995, se institucionalizó la figura de holding para sociedades financieras y no financieras bajo la denominación de grupo ya mencionada. Así, se entiende por conglomerado financiero, el conjunto de entidades vigiladas por la SFC y sus filiales, y subsidiarias en el exterior que ejerzan la actividad financiera, bursátil o aseguradora. Este cambio en el modelo de organización del sistema financiero ha permitido que las entidades reguladoras tengan más control sobre la regulación y supervisión de los conflictos de interés que se pudieran generar, la posible existencia de piramidación de capital y la presencia del riesgo de contagio. (Banco de la República, 2013)

Según el Banco de la República (2013), con la intención de mantener la estabilidad del sistema financiero, en Colombia se estableció la Red de Seguridad del Sistema Financiero (RSF), la cual es un conjunto de normas, procedimientos, mecanismos e instituciones que buscan facilitar la relación entre las entidades responsables del buen funcionamiento del sistema financiero, esto con el fin de reducir la probabilidad de quiebra de las entidades del sistema financiero. Las entidades encargadas de regular el sistema financiero son:

- **Ministerio de Hacienda y Crédito Público (MHCP):** define las políticas generales de regulación del sistema financiero y del mercado de valores.
- **Superintendencia Financiera de Colombia (SFC):** supervisa y adopta políticas de inspección y vigilancia en cuanto a solvencia y liquidez.
- **Autorregulador del Mercado de Valores (AMV):** ejerce funciones de regulación y supervisión disciplinaria. Desempeña una labor complementaria a la del MHCP y la SFC.
- **Fondo de Garantías de Instituciones Financieras (Fogafín):** su objetivo es administrar el seguro de los depósitos y las operaciones de fortalecimiento patrimonial de los EC (excepto de las cooperativas financieras)

- **Fondo de Garantías de Entidades Cooperativas (Fogacoop):** su objetivo es administrar el seguro de los depósitos y las operaciones de fortalecimiento patrimonial de las cooperativas
- **Banco de la República:** su papel está relacionado con las condiciones para otorgar liquidez a las entidades financieras, además de ser el prestamista de última instancia para las EC. Asimismo monitorea los posibles riesgos a los que se enfrenta el sistema financiero y aquellos relacionados con el sistema de pagos.

Es importante aclarar que la Ley 795 de 2003 del Banco de la República (2013), la cual se encuentra reglamentada por el Decreto 1044 de 2003, creó el Comité de Coordinación para el Seguimiento al Sistema Financiero (CCSSF), el cual está integrado por representantes de algunas de las entidades mencionadas anteriormente (no incluye al representante del AMV ni al de Fogacoop). Este comité actúa como instrumento de enlace y coordinación, por lo cual le fueron asignadas actividades tales como: divulgar información relevante para el ejercicio de las funciones de las entidades que lo componen, promover de manera oportuna y coordinada las actuaciones definidas en el comité para cada entidad, solicitar a las entidades del Estado la información que considere necesaria para cumplir con sus objetivos, realizar estudios técnicos y jurídicos que fundamenten la expedición de normas de regulación o supervisión de las entidades, entre otras.

La cuantificación del riesgo se ha convertido en una de las preocupaciones centrales de los investigadores y operadores en finanzas ya que cada vez sienten mayor necesidad de responder a la normatividad establecida por las entidades reguladoras nacionales e internacionales. En el contexto de las finanzas, cuando se habla de riesgo se hace referencia a la posibilidad de pérdidas causadas por variaciones de los factores que afectan el valor de un activo. Por esa razón, según Arbeláez et al. (2006) es importante que se identifiquen, se midan, se controlen, y se haga un monitoreo continuo de los diversos tipos de riesgo a los que están expuestas las entidades en el desarrollo cotidiano de sus actividades. Además de esto, según la Compañía Aseguradora de Finanzas S.A (2011) un riesgo se define como cualquier situación, circunstancia, evento, amenaza, acto u omisión que pueda en algún momento impedir el logro de los objetivos estratégicos de la compañía. Para el Sistema de Administración de Riesgo- SARO (2011) los diferentes tipos de riesgo son:

1. **Riesgo crédito**: posibilidad de incurrir en pérdidas por el no pago o pago inoportuno de las obligaciones de usuarios, intermediarios y otras compañías.
2. **Riesgo de mercado:** posibilidad de incurrir en pérdidas por cambios en el entorno como tasas de interés, tasas de devaluación u otros parámetros.
3. **Riesgo de liquidez**: imposibilidad de adquirir los fondos necesarios para cubrir obligaciones de corto plazo.
4. **Riesgo de suscripción**: incurrir en pérdidas como consecuencia de tener políticas o prácticas inadecuadas en el diseño de productos o colocación de los mismos.
5. **Riesgo legal**: pérdidas por incumplimiento de normas legales.

6. **Riesgo estratégico**: pérdidas como consecuencia de la imposibilidad de implementar apropiadamente los planes de negocio, estrategias o decisiones de mercado, incapacidad para adaptarse a los cambios del entorno.
7. **Riesgo reputacional**: pérdidas derivadas por la celebración de acuerdos sobre los cuales recaiga una publicidad negativa, realización de prácticas que puedan derivar en demandas legales y pérdida de credibilidad del público.
8. **Riesgo de lavado de activos y financiación del terrorismo**: pérdida o daño que puede sufrir una entidad por ser utilizada como instrumento para el lavado de activos o financiación del terrorismo.
9. **Riesgo operacional**: posibilidad de incurrir en pérdidas por deficiencias, fallas o inadecuaciones, en el recurso humano, los procesos, la tecnología, la infraestructura o por la ocurrencia de acontecimientos externos.

Según la Superintendencia Financiera (2007), las entidades deben establecer las políticas, objetivos, procedimientos y estructuras para la administración del riesgo operativo donde el sistema debe estar alineado con los planes estratégicos de la entidad financiera. Así, en la administración del riesgo operativo, las empresas deben desarrollar las siguientes etapas si pretenden realizar una buena gestión de este riesgo.

1. **Identificación**: reunir información sobre cada uno de los procesos y procedimientos teniendo claridad sobre los objetivos de cada uno.

2. **Medición**: Se debe realizar en términos de probabilidad de ocurrencia e impacto en caso de que se materialice el evento de riesgo. Si va a ser cuantitativa se deben tener datos históricos de por lo menos 1 año.
    - Riesgo inherente
    - Efectividad de los controles
    - Riesgo residual

3. **Control**: medidas para mitigar el riesgo inherente con el fin de disminuir su probabilidad de ocurrencia o impacto.

4. **Monitoreo**: hacer seguimiento efectivo y facilitar la detección y corrección de las deficiencias. Tiene que tener una periodicidad mínima y se debe realizar por medio de indicadores que evidencien los potenciales eventos del riesgo operativo. (Superintendencia Financiera de Colombia, 2006)

Asimismo, la SFC (2007) indica que las entidades deben analizar los factores de riesgo ya que estos son las fuentes generadoras de riesgos operativos que pueden o no generar pérdidas para las empresas. Estos factores se pueden clasificar en internos o externos como se menciona a continuación:

1. **Riesgos internos**

    - **Recurso humano:** conjunto de personas vinculadas directa o indirectamente con la ejecución de los procesos de la entidad.

- **Procesos:** actividades que transforman los elementos de entrada en productos o servicios con el fin de satisfacer una necesidad.
- **Tecnología:** herramientas utilizadas para soportar los procesos de la entidad
- **Infraestructura:** elementos que brindan apoyo al funcionamiento de una organización.

2. **Riesgos externos:** situaciones ocasionadas por la fuerza de la naturaleza o por terceros, no son controlables por la entidad.

Por otra parte, los riesgos operativos se clasifican de la siguiente manera:

- **Fraude interno**: algún tipo de actuación de empleados o terceros vinculados contractualmente con la compañía. Incluye fraudes, robos, sobornos, etc.
- **Fraude externo**: pérdidas derivadas de algún tipo de actuación de personas ajenas que buscan afectar la compañía. Incluye robos, falsificación y ataques informáticos
- **Fallas tecnológicas**: fallos en los sistemas de cómputo, comunicaciones, hardware o software de la compañía. Incluye caídas de sistemas por tiempos prolongados, daños en líneas telefónicas, pérdida de información, virus informático
- **Ejecución y gestión de procesos**: errores en el procedimiento de operaciones. Incluye captura de transacciones, ejecución y mantenimiento, monitoreo y reporte, entrada de documentación de clientes, gestión de cuentas de clientes.
- **Relaciones laborales y seguridad en el puesto de trabajo**: pago de reclamaciones por daños personales y casos relacionados con discriminación en el trabajo.
- **Daños a activos materiales**: pérdidas derivadas de daños o perjuicios a activos físicos. Incluye incendios, terremotos, actos terroristas y falta de mantenimiento.
- **Clientes, productos y prácticas empresariales**: incumplimiento involuntario o negligente de una obligación profesional. Incluye competencia desleal, falsos beneficios en productos, perjuicios a clientes.

(Superintendencia Financiera de Colombia, 2006)

Teniendo en cuenta lo anterior, el Comité de Supervisión Bancaria de Basilea (BCBS, por sus siglas en inglés), se creó para estandarizar y regular los diferentes tipos de riesgo con el fin de aumentar la calidad de supervisión bancaria a nivel mundial. Este es el principal órgano normativo internacional para la regulación prudencial de los bancos, pues constituye un foro de cooperación en materia de supervisión bancaria. Su objetivo es mejorar la regulación, la supervisión y las prácticas bancarias en todo el mundo con el fin de afianzar la estabilidad financiera (Comité de Supervisión Bancaria de Basilea, 2013). Este lleva a cabo su mandato a través del desarrollo de las siguientes funciones, las cuales se especifican en la carta estatutaria del mismo.

- Intercambiar información sobre la evolución del sector bancario y los mercados financieros, con el fin de detectar riesgos actuales o incipientes para el sistema financiero mundial.

- Compartir asuntos, estrategias y técnicas de supervisión para propiciar un entendimiento común y mejorar la cooperación internacional.
- Establecer y promover normas internacionales, directrices y buenas prácticas en materia de regulación y supervisión bancaria.
- Abordar las lagunas de regulación y supervisión que planteen riesgos para la estabilidad financiera.
- Vigilar la aplicación de las normas del BCBS en los países miembros y otros países, con el fin de asegurar su aplicación oportuna, uniforme y eficaz, y contribuir al fomento de condiciones equitativas entre los bancos con actividades internacionales.
- Consultar con los bancos centrales y las autoridades de supervisión bancaria no pertenecientes al BCBS para tener en cuenta su opinión en el proceso de formulación de políticas y fomentar la aplicación de las normas, directrices y buenas prácticas del BCBS en los países no miembros.
- Coordinar y cooperar con otras entidades normativas y organismos internacionales del sector financiero, en particular aquellos que promueven la estabilidad financiera. (Carta estatutaria, 2013)

El BCBS ha desarrollado directrices y estándares como son el Estándar Internacional sobre Medidas y Normas de Capital (Acuerdos de Basilea), los Principios Básicos para una Supervisión Bancaria Eficaz (*Core Principles*) y el Concordato sobre Supervisión Transfronteriza (Banco de España). De acuerdo con Management Solutions (2012), los Acuerdos de Basilea son recomendaciones sobre regulación y supervisión bancaria por medio de los cuales, el Comité de Basilea pretende asegurar la capacidad de los bancos de absorber las pérdidas derivadas de los riesgos inherentes a su actividad.

Basilea III, último acuerdo publicado por la entidad en el año 2010 dejó clara la necesidad de dictar esquemas de administración del riesgo operativo pues el desarrollo de las prácticas bancarias sugiere que, aparte de los riesgos de crédito, de tipo de interés y de mercado, pueden ser considerados, a efectos de supervisión, otros riesgos, como es el caso del operacional. Anteriormente el riesgo operativo se gestionaba mediante una auditoría interna o control interno, sin llegar a otorgarle una unidad específica dentro del área de riesgos; sin embargo, hoy en día se busca la gestión integral del riesgo operacional incluyendo la utilización de metodologías cuantitativas (Jiménez Rodríguez & Matín Marín, 2005). Por lo anterior, el Comité de Supervisión Bancaria de Basilea con la intención de facilitar la gestión del riesgo operacional, clasificó el mismo como se puede evidenciar en la siguiente tabla.

Tabla 1. Categorías y tipos de eventos de pérdidas asociados a riesgo operacional.

Categoría de Tipo de Eventos (nivel 1)	Definición	Categoría (nivel 2)	Ejemplos de actividades (Nivel 3)
Fraude interno	Pérdidas derivadas de algún tipo de actuación encaminada a defraudar, apropiarse de bienes indebidamente o soslayar regulaciones, leyes o políticas empresariales (excluidos los eventos de diversidad / discriminación) en las que se encuentra implicada, al menos, una parte interna a la empresa	Actividades no autorizadas	i) Operaciones no reveladas intencionalmente; ii) Operaciones no autorizadas con pérdidas monetarias; y iii) Valoración errónea intencional de posiciones
		Hurto y fraude	i) Fraude / fraude crediticio/ depósitos sin valor Hurto / extorsión / malversación / robo; ii) Apropiación indebida de activos; iii) Destrucción dolosa de activos; iv) Falsificación; v) Utilización de cheques sin fondos; vi) Contrabando; vii) Apropiación de cuentas, de identidad, etc.; viii) Incumplimiento / evasión intencional de impuestos; ix) Soborno / cohecho; y x) Abuso de información privilegiada
Fraude externo	Pérdidas derivadas de algún tipo de actuación encaminada a defraudar, apropiarse de bienes indebidamente o soslayar la legislación, por parte un tercero	Hurto y fraude	i) Hurto/ robo; ii) Falsificación; y iii) Utilización de cheques sin fondos
		Seguridad de los sistemas	i) Daños por ataques informáticos; y ii) Robo de información con pérdidas monetarias
Relaciones laborales y seguridad en el puesto de trabajo	Pérdidas derivadas de actuaciones incompatibles con la legislación o acuerdos laborales, sobre higiene o seguridad en el trabajo, sobre el pago de reclamaciones por daños personales, o sobre casos relacionados con la discriminación	Relaciones laborales	i) Cuestiones relativas a remuneración, prestaciones sociales, extinción de contratos; y ii) Organización laboral
		Higiene y seguridad en el trabajo	i) Imposibilidad en general (resbalones, caídas, etc.); ii) Casos relacionados con las normas de higiene y seguridad en el trabajo; y iii) Indemnización a los trabajadores
		Diversidad y discriminación	Todo tipo de discriminación
Incidencias en el negocio y fallos en los sistemas	Pérdidas derivadas de interrupción en los negocios o por fallas en los sistemas	Sistemas	i) Hardware; ii) Software; iii) Telecomunicaciones; y iv) Interrupción / incidencias en el suministro
Daños a activos materiales	Pérdidas derivadas por daños o perjuicios a activos materiales como consecuencia de desastres naturales u otros eventos	Desastres y otros acontecimientos	i) Pérdidas por desastres naturales; ii) Pérdidas humanas por causas externas (terrorismo, vandalismo)
Clientes, productos y prácticas empresariales	Pérdidas derivadas del incumplimiento involuntario o negligente de una obligación profesional frente a clientes concretos (incluidos requisitos fiduciarios y de adecuación), o de la naturaleza o diseño de un producto	Adecuación, divulgación de información y confianza	i) Abusos de confianza / incumplimiento de pautas; ii) Apropiamiento / divulgación de información; ii) Violación de la privacidad de clientes minoristas; iii) Quebrantamiento de privacidad; iv) Ventas agresivas; v) Pérdidas de cuentas; vi) Mal uso de información confidencial; y vii) Responsabilidad del prestamista
		Prácticas empresariales o de mercado impropias	i) Prácticas anti-competencia; ii) Prácticas impropias comerciales y de mercado; iii) Manipulación del mercado; iv) Comercialización de información privilegiada a favor de la empresa; v) Actividades no autorizadas; y vi) Lavado de dinero
		Productos defectuosos	i) Defectos del producto; y ii) Error de modelo
		Selección, patrocinio y riesgos	i) Fallida investigación a clientes según los protocolos; y ii) Superación de los límites de exposición frente a clientes
		Actividades de asesoramiento	Litigios sobre resultados de las actividades de asesoramiento
Ejecución, entrega y gestión de procesos	Pérdidas derivadas de errores en el procesamiento de operaciones o en la gestión de procesos, así como de relaciones con contrapartes comerciales y proveedores	Recepción, ejecución y mantenimiento de operaciones	i) Comunicación defectuosa; ii) Errores de introducción de datos, mantenimiento o descarga; iii) Incumplimiento de plazos o de responsabilidades; iv) Ejecución errónea de modelos / sistemas; v) Error contable / atribución a entidades erróneas; vi) Errores en otras tareas; vii) Fallo en la entrega; viii) Fallo en la gestión del colateral; y ix) Mantenimiento de datos de referencia
		Seguimiento y Monitoreo	i) Incumplimiento en la obligación reportar; y ii) Inexactitud de informes externos (incurriendo en pérdidas)
		Aceptación de clientes y documentación	i) Extravío de autorizaciones / rechazos de clientes; y ii) Documentos jurídicos inexistentes / incompletos
		Gestión de cuentas de clientes	i) Acceso no autorizado a cuentas; ii) Registros incorrectos de clientes (incurriendo en pérdidas); y iii) Pérdida o daño de activos de clientes por negligencia
		Contrapartes comerciales	i) Fallos con contrapartes no-clientes; y ii) Otros litigios con contrapartes distintas de clientes
		Distribuidores y proveedores	i) Subcontratación; y ii) Litigios con distribuidores

Fuente: (Riesgo Operacional: Conceptos y Mediciones, 2009)

Los acuerdos de Basilea II y III tienen como finalidad mejorar la seguridad y solvencia de los sistemas financieros, y ser una norma de adecuación de capital más sensible al riesgo de las operaciones bancarias. El acuerdo se basa en tres pilares: los requisitos mínimos de capital en función de los riesgos asumidos, la revisión supervisora y la disciplina de mercado. El capital regulatorio puede definirse como los recursos de los que debe disponer la entidad para absorber las posibles pérdidas a las que puede enfrentarse debido a los eventos de riesgo, la revisión supervisora se refiere a los diferentes modelos de gestión del riesgo, y la disciplina de mercado frente a la divulgación de información sobre riesgo operacional. Los requerimientos mínimos de capital aplican de igual forma en Basilea II y III para el riesgo operacional, de crédito, de mercado y de liquidez, con el fin de asegurar que las entidades bancarias mantengan el capital necesario para dar cobertura al riesgo global. (Pakhchanyan, 2016)

Partiendo de la premisa que el riesgo operativo puede poner en peligro la estabilidad de los sistemas financieros, el Comité de Supervisión Bancaria de Basilea propone tres métodos generales para el cálculo del capital regulatorio de cobertura del riesgo operativo, estos métodos varían por su sofisticación y sensibilidad al riesgo, y son los siguientes (Mora, 2008):

1. Enfoque del Indicador Básico **(BIA, Basic Indicator Approach):** calcula el capital regulatorio como un porcentaje fijo de un indicador de exposición de la empresa al riesgo operativo, generalmente el indicador utilizado son los ingresos brutos. La proporción fijada por Basilea es del 15% (factor alfa) sobre el promedio de los ingresos brutos anuales de los últimos tres años. (Guijarro, 2013)

2. Enfoque Estándar **(SA, Standardised Approach)**: se calcula el capital regulatorio para cada una de las líneas de negocio del banco aplicando distintos porcentajes al indicador de exposición para obtener al final el requerimiento total como la suma de los requerimientos de cada línea. El factor beta por el cual se multiplican los ingresos brutos, estima la exposición que tiene cada línea de negocio, y permite calcular la provisión de capital para cada una de estas. De esta forma los bancos deberán retener un capital regulatorio correspondiente al promedio de las ganancias positivas de los tres años anteriores multiplicadas por un porcentaje fijo. (Nieto Giménez & Gómez Fernández, 2006) Los factores beta son los siguientes:

Tabla 2. Factores beta para líneas de negocio

Líneas de negocio	Factores Beta
Financiación empresarial o corporativa (β1)	18%
Negociación y ventas (β2)	18%
Pagos y liquidación (β3)	18%
Servicios de agencia (β4)	15%
Administración de activos (β5)	12%
Intermediación minorista (β6)	12%
Banca minorista (β7)	12%
Banca comercial (β8)	15%

Fuente: (Romero, 2009)

3. Enfoques de Medición Avanzada **(AMA, Advanced Measurement Approach):** en este enfoque se establecen unas directrices generales para dejar libertad a las entidades financieras de diseñar su propio modelo de medición y gestión del riesgo operativo. El enfoque AMA permite establecer de forma más detallada el perfil de riesgo específico, que finalmente se traduce en cuantificar de forma más precisa los requisitos de capital (Moosa, 2007). Adicionalmente, dentro de este enfoque el Comité admite tres modelos alternativos:

   a. *Enfoque de Medición Interna* ***(Internal Measurement Approach, IMI)***

   Se utilizan los datos de pérdidas internas del banco como entradas para el cálculo del capital regulatorio. En este enfoque el riesgo operacional es categorizado basado en una matriz compuesta por las líneas de negocio y tipos de eventos. Para cada combinación de línea de negocio y tipo de evento se estima el capital requerido basado en las pérdidas esperadas y un factor fijo gamma (Federal Reserve Bankof Boston, 2014). El capital de requerimiento total es la suma de los requerimientos particulares de las combinaciones de cada línea de negocio y evento de riesgo, sin embargo, Chaudhuri & Ghosh (2016) mencionan que actualmente no hay suficientes datos a nivel de la industria para poder calcular la carga de capital bajo este enfoque, así, la industria deberá reunir datos adecuados durante varios años para que este enfoque sea viable.

   b. *Enfoque de la Distribución de Pérdidas* ***(Loss Distribution Approach, LDA)***

   Es el enfoque más utilizado en la práctica bancaria para determinar el capital requerido para cubrir las pérdidas por riesgo operacional. En este se analizan los datos de pérdidas históricos desde la frecuencia con la que se repiten los sucesos y la severidad o cuantía de la pérdida. Cada entidad define un umbral de captura de los datos y un umbral de modelización, el primero es el importe mínimo del evento operacional a partir del cual la entidad empieza a capturar

sus datos; y el segundo es el importe a partir del cual la entidad modela los datos. Una vez definidos los umbrales se ajustan las frecuencias y severidad a una distribución estadística, y finalmente se halla una distribución total de las pérdidas a partir de las precedentes. (Di Pietro, Irimia-Diéguez, & Oliver-Alfonso, 2012)

Una vez se determina la función de pérdidas agregada se halla el OpVar, el cual se calcula como el cuantil 0.999 de la distribución, y que determina la máxima pérdida probable en unidades monetarias por riesgo operacional que podría esperarse en un horizonte de un año, con una confianza del 99.9%. (Moosa, 2007)

c. *Cuadros de Mandos* ***(Scorecard Approach)***

Son modelos de gestión basados en indicadores financieros y de riesgo. En los indicadores se identifican variables representativas del funcionamiento de la entidad en aquellos puntos donde pueden ocasionarse pérdidas operacionales, permitiendo la identificación, control y seguimiento del riesgo. Este enfoque está basado en la experiencia y opinión de expertos de las entidades, quienes periódicamente envían información sobre la calidad del sistema de control interno y externo, para luego utilizar estas apreciaciones en la calificación de cada evento de riesgo según su frecuencia, controles y severidad. (Giudici, 2007)

Respecto los enfoques anteriores, es pertinente mencionar que debido a la flexibilidad que otorga el Comité para la implementación de los enfoques avanzados, se ha venido generado en la práctica resultados diferentes en los requerimientos de capital, aún en entidades con perfiles de riesgo operacional iguales. En el enfoque LDA, que como se mencionó es el más utilizado por las entidades financieras, tal variabilidad se debe al tipo de umbral de pérdidas y las distribuciones estadísticas elegidas para el modelo. El problema que supone lo anterior es que se podría dar lugar a una estimación baja o una sobreestimación del capital regulatorio, lo que implica un costo de oportunidad. Así, se ha puesto en manifiesto que la medición del riesgo operacional sigue siendo una cuestión abierta, pues dejar a total elección de los bancos la metodología puede conllevar a mediciones imprecisas. (Di Pietro, Irimia-Diéguez, & Oliver-Alfonso, 2012)

Comité de Supervisión de Basilea (2016) considerando la desventaja que evidencian los métodos avanzados, propone un nuevo método que tiene como objetivo estandarizar la medición de riesgo operacional al otorgar una mayor sensibilidad al riesgo y una mayor comparabilidad. El Método de Medición Estandarizado (SMA) permite incorporar las propias experiencias de pérdidas operativas de los bancos al tener en cuenta los siguientes elementos:

1. **Indicador de Negocios (BI):** es un proxy financiero que revela la exposición al riesgo operacional teniendo en cuenta los datos de pérdidas específicas de la entidad, y la experiencia histórica del banco. En la práctica se define como la suma de ingresos y gastos operacionales. La entidad que no compre productos de terceros, solo debe incluir el rubro de ingresos, obteniendo así una menor carga de capital. (Basel Committee on Banking Supervision, 2016)

2. **Componente del Indicador de Negocio (BI Component):** este fue calibrado usando la data recolectada en el Estudio de Impacto Cuantitativo (QIS) realizado por el comité en la segunda mitad del año 2015. Partiendo de esta calibración realizada, la cual refleja la experiencia generalizada de los bancos del estudio, el componente BI refleja la exposición a pérdidas operacionales del promedio de lo reflejado en el QIS para un banco dado un tamaño de BI específico. (Basel Committee on Banking Supervision, 2016)

   Bajo este método los bancos son divididos en 5 grupos de acuerdo al tamaño de su indicador de negocios, a su vez dependiendo de ese indicador de negocio se asigna un componente de BI específico como se muestra a continuación.

Tabla 3. Clasificación según BI

Bucket	BI Range	BI Component
1	€0 to €1 bn	0.11*BI
2	€1 bn to €3 bn	€110 m + 0.15(BI – €1 bn)
3	€3 bn to €10 bn	€410 m + 0.19(BI – €3 bn)
4	€10 bn to €30 bn	€1.74 bn + 0.23(BI – €10 bn)
5	€30 bn to +∞	€6.34 bn + 0.29(BI – €30 bn)

Fuente: (Basel Committee on Banking Supervision, 2016)

3. **Multiplicador Interno de Pérdida y Componente de Pérdida (Loss Component**): el componente de pérdidas tiene en cuenta las pérdidas del banco y ajusta la sensibilidad al riesgo del método. Este componente se introduce en el Método de Medición Estandarizada mediante el multiplicador interno de pérdidas de la siguiente forma:

$$Internal\ Loss\ Multiplier = Ln(e^1 - 1 + \frac{Loss\ Component}{BI\ Component})$$

   El componente de pérdidas distingue entre eventos con una severidad superior a 10 y 100 millones de euros, y eventos de pérdidas menores a esas cantidades para diferenciar entre bancos con diferentes colas de distribuciones de pérdidas, pero con

similar promedio total de pérdidas. En teoría los bancos deben usar datos de pérdidas de un período mínimo de 10 años, sin embargo, en el período de transición a este método, aquellos bancos que no tienen recolectada esta cantidad de datos deben tener un mínimo de 5 años de registros de datos de pérdidas operacionales. Si no se cuenta con este historial, la entidad deberá trabajar solo con el BI. (Basel Committee on Banking Supervision, 2016)

Teniendo en cuenta los elementos anteriores, el requerimiento de capital de riesgo operativo se calcula de la siguiente manera:

$$SMA = \begin{cases} BI\ Component, if\ Bucket\ 1 \\ 110\ Mln + (BI\ Component - 110 Mln) * Ln(\exp(1) - 1 + \frac{Loss\ Component}{BI\ Component}), If\ Buckets\ 2-5 \end{cases}$$

$$BI\ Component = \begin{cases} 0.11 * BI, if\ Bucket\ 1 \\ 110 Mln + 0.15(BI - 1Bln), if\ Bucket\ 2 \\ 410 Mln + 0.19(BI - 3Bln), if\ Bucket\ 3 \\ 1.74 Bln + 0.23(BI - 10Bln), if\ Bucket\ 4 \\ 6.34 Bln + 0.29(BI - 30Bln), if\ Bucket\ 5 \end{cases}$$

Y:

$$\begin{aligned} Loss\ Component = {} & 7 * Average\ Total\ Anual\ Loss + 7 \\ & * Average\ Total\ Annual\ Loss\ only\ incluiding\ loss\ events\ above\ \$10\ million + 5 \\ & * Average\ Total\ Annual\ Loss\ including\ loss\ events\ above\ \$100\ million \end{aligned}$$

Todos los métodos anteriormente mencionados buscan ser coherentes con las características del riesgo operacional con el fin de obtener un valor en riesgo coherente con el perfil de riesgo operacional de la entidad. El riesgo operativo se caracteriza por ser endógeno, es decir que varía significativamente basado en las operaciones internas de cada compañía, es por esto que para su cálculo se requiere data específica de la compañía y que esta sea representativa respecto al entorno actual del riesgo. Asimismo, este tipo de riesgo se administra con base en los cambios en procesos, tecnología, personas, organización y cultura; esta característica conlleva a que este riesgo requiera ser modelado como una función de decisiones operacionales, y que se requiera comprender los factores causales del mismo. Finalmente, otra característica que determina la medición de este riesgo es el hecho que este tiene distribuciones sesgadas, es decir, de cola larga. (Shah, 2001)

Dado que el enfoque del proyecto es el sistémico y que una de las características del riesgo operativo hace referencia a la necesidad de comprender los factores causales del riesgo operacional, resulta pertinente esclarecer los conceptos y metodologías relacionadas; para esto se tiene en cuenta que las aproximaciones del enfoque sistémico se basan en la teoría de sistemas, y esta a su vez se relaciona con la cibernética y la dinámica de sistemas. Para

empezar, según Speedding (1979) un sistema es un conjunto de componentes con límites específicos que funcionan recíprocamente para lograr un propósito común, y que reaccionan juntos al ser estimulados por influencias externas. (FAO, s.f.) Cabe mencionar que en la literatura pueden encontrarse variadas definiciones sobre sistemas, pero todas apuntan a que un sistema es un conjunto de elementos o individuos que forman parte de un todo organizado, que interactúan entre sí y tienen conductas coherentes orientadas hacia un mismo fin. (BVSDE:Colombia, 2010)

La concepción de los objetos como un todo, y el todo como mucho más que la suma de las partes (principio de sinergia) se deriva de Aristóteles, el cual introduce el principio general del holismo, en su metafísica. El holismo es la idea de que todas las propiedades de un sistema dado, ya sea biológico, químico, social, económico o mental, no pueden ser determinados o explicados por sus partes integrantes de forma separada, sino que es el sistema como un todo el que determina el comportamiento de sus partes. En suma, en este principio se le otorga la mayor importancia al todo, y a la interdependencia de sus partes (Clemente, 2010). No obstante, en la década de 1940 Ludwig von Bertanffy da una mayor consistencia y formalización a lo planteado por Aristóteles con el planteamiento de la Teoría General de Sistemas, en la cual busca proporcionar un marco teórico y práctico a las ciencias naturales y sociales diferente al mecanicismo de la época, que proponía la división del mundo en partes. (Estaire, 2012)

La Teoría de Sistemas, según la organización internacional Principia Cybernetica (2000), especialmente conocida por su página web de Principia Cybernetica Web, la teoría de sistemas es el estudio interdisciplinario de la organización abstracta de los fenómenos, independiente de sus sustancia, tipo o existencia temporal o espacial. Esta teoría investiga tanto los principios comunes a todas las entidades complejas como los modelos que pueden utilizarse para describirlas (Heylighen & Joslyn, 1992). Dicho de otro modo, la teoría de sistemas estudia la organización de las partes de un sistema y sus relaciones en función de su conexión con el todo, y precisamente observar un problema de este modo es conocido como enfoque sistémico. Kenneth Boulding otro de los precursores de la teoría de sistemas, establece que esta teoría tiene como finalidad unificar los enfoques organicistas, matemático y tecnológico de un sistema, para encontrar elementos comunes a todos los enfoques y definir un conjunto de proposiciones y leyes aplicables a todo tipo de sistemas. Los componentes de estos sistemas cumplen funciones de información, realimentación (feedback), evolución y control. (Coll, 2007)

Los diagramas de bucles causales son las estructuras que se basan en el concepto de feedback, estos son fases construidas mediante la unión de variables claves, indicando la relación causal entre ellas para articular el entendimiento de situaciones dinámicas e interconectadas. La utilidad de estas estructuras está en que permiten ir más allá de los eventos individuales para dar lugar a un nivel sistémico de entendimiento. Además, facilitan la visualización de variables y su relación en el tiempo, permiten evaluar los estados

actuales y patrones de relaciones, y realizar suposiciones sobre comportamientos futuros. (Williams & Hummelbrunner, 2011)

Los bloques de construcción de los diagramas de bucles causales son los bloques de retroalimentación los cuales son secuencias cerradas de causas y efectos. Existen dos tipos de bucles de feedback:

1. **Feedback positivo o de refuerzo**: todas las variables responden al comportamiento de la otra en la misma dirección.

2. **Feedback negativo o de balance:** ocurre cuando al menos una variable del sistema responde de manera contraria al cambio en otra variable. (Williams & Hummelbrunner, 2011)

Para la construcción de diagramas de bucles causales se deben seguir cuatro etapas:

1. **Identificar elementos relevantes:** se debe definir claramente la situación de interés (límites), el horizonte de tiempo y determinar las variables relevantes para el problema a resolver, estas últimas deben variar en el tiempo.

2. **Determinar relaciones:** establecer relaciones causales positivas o negativas entre las variables ilustradas con conexiones mediante flechas, lo cual indica la relación de influencia, y un símbolo al final de la línea indicando el tipo de causalidad.

3. **Formar bucles de feedback:** se verifica que todas las variables estén conectadas y formen círculos cerrados de influencia, el resultado debe ser una red de causas y efectos formada por varios bucles de feedback interconectados. Las causas y efectos del diagrama no pueden considerarse de forma unívoca, sino que depende de la posición, lo que alguien considera causa, otra puede considerarlo efecto.

4. **Analizar bucles:** se analiza el diagrama en función del número de bucles, longitud de las conexiones y conexión de las variables. (Williams & Hummelbrunner, 2011)

Debido a que los sistemas sociales están conformados de bucles de retroalimentación, la mente humana no es capaz de interpretar totalmente su comportamiento, y, por tanto, las herramientas de la dinámica de sistemas son valiosas para estudiar este tipo de sistemas. La dinámica de sistemas es un enfoque para la comprensión del comportamiento dinámico de un sistema, en particular de un sistema social, y fue originalmente desarrollada en 1950 en el MIT por Jay Forrester. Su objetivo era hacer uso de su experiencia en ciencia e ingeniería para encargarse de las diferentes problemáticas que enfrentan las organizaciones; y en la actualidad, existen diferentes softwares disponibles para crear este tipo de modelos. (Williams & Hummelbrunner, 2011)

El concepto de la dinámica de sistemas está basado en la idea de los sistemas están compuestos por elementos que toman valores en puntos determinados de tiempo (stock), y que pueden cambiar mediante flujos de entrada o de salida. Así, el comportamiento dinámico de un sistema se explica mediante las relaciones entre variables de stock y flujo expresadas en un diagrama de stock-flow, donde las variables de stock al ser las que acumulan los eventos pasados, constituyen la memoria del sistema. De manera general un diagrama de stock-flow se compone de:

- **Variables stock (acumulador):** cantidades que puedan acumular o disminuir en el tiempo, los stocks casi siempre son visibles y fáciles de identificar. En el diagrama se representan como cajas rectangulares.

- **Variables de flujo (Tasas):** describen el cambio en las variables de stock, por tanto, debe hacerse una distinción entre entradas y salidas. Pueden ser valores absolutos o índices por unidades de tiempo. Son representadas en el diagrama como una línea doble direccional y una válvula.

- **Límites:** una nube simboliza los límites del sistema en consideración, son factores exógenos al modelo.

- **Variables auxiliares**: son variables que no tienen influencia directa en el sistema pero que sirven para ilustrar relaciones entre variables. Se representan por otros símbolos o pueden ser dibujadas como diagramas de influencia o bucles de retroalimentación.
  (Williams & Hummelbrunner, 2011)

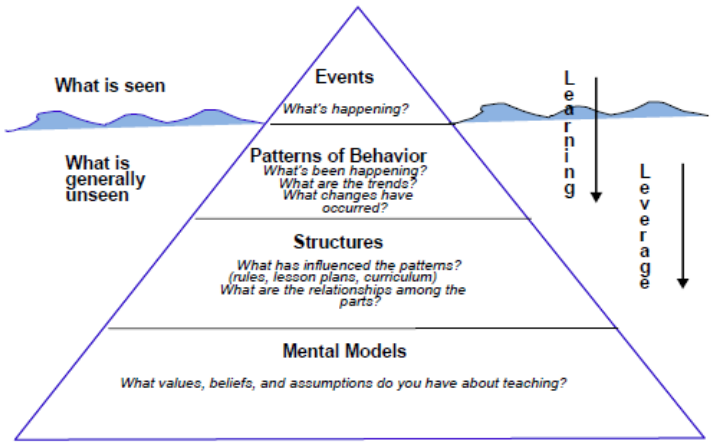
Complementando lo anterior, la formulación de un modelo dinámico contiene al igual que los diagramas de bucles causales cuatro etapas. El proceso de la dinámica de sistemas comienza identificando una situación de interés ya sea un problema o necesidad. Una identificación clara de la situación es crucial para el éxito de una investigación con dinámica de sistemas, y del mismo modo que con los diagramas de bucles causales, no se debe pretender modelar todo el contexto donde la situación de interés está situada, sino que deben definirse los límites y permanecer focalizados en aquellos elementos relevantes para el problema que será modelado. Seguidamente, se desarrolla una hipótesis de la dinámica que explica el núcleo de la situación de interés, algunas veces esto es realizado primero mediante diagramas de bucles causales y luego trasladado al diagrama de stock-flow.

Posteriormente se procede a la construcción del modelo, donde se recomienda empezar con las relaciones de mayor importancia o las más visibles entre variables. También debe considerarse que las variables de flujo y stock deben cuantificarse, y la relación entre las variables debe estar exactamente definida, lo que quiere decir que, por cada relación entre variables, una función matemática debe definirse para representar la relación lineal o no lineal entre las variables. En la construcción del modelo de simulación debe asegurarse que

todos los elementos queden ensamblados, definidos y expresados en relaciones matemáticas, además debe verificarse que los valores de stock solo sean cambiados por los de flujo, que cada flujo esté conectado a un stock, y que los stocks no estén conectados directamente entre ellos. Finalmente, una vez el modelo este elaborado se procede a correr las simulaciones para modelar o explorar las consecuencias de diferentes valores de intervención, tiempos, retrasos y retroalimentaciones. (Williams & Hummelbrunner, 2011)

La teoría del modelo del iceberg propuesto por Daniel Kim (1996) es una herramienta de pensamiento sistémico en la cual se sustenta lo que aquí se propone, plantear un modelo de gestión de riesgo operativo que involucre la estructura causal de los patrones de riesgo. La teoría utiliza la analogía del iceberg para ilustrar que, así como en este elemento el 90% de su volumen está oculto a la vista, en el estudio de un problema o fenómeno, la mayoría de sus elementos están escondidos, y por tanto para alcanzar una comprensión profunda sobre lo que nos rodea, debe explorarse mucho más allá de la superficie. De esta forma, el autor propone la existencia de 4 niveles de conocimiento: eventos, patrones de comportamiento, estructuras de soporte y modelos mentales. (Huigens, 2005)

Ilustración 1. Modelo del Iceberg



Fuente: (Goodman, 2002)

Eventos: marcadores en el tiempo donde múltiples variables son observadas. La mayor parte del mundo transcurre en el nivel de eventos y generalmente se presentan en la cotidianidad como problemas a solucionar. Cuando se observan los problemas a este nivel las soluciones tienen a ser reactivas, es decir, devuelven el problema en un determinado tiempo y posiblemente con nuevos elementos de análisis.

Patrones: cambios en las variables que ocurren en el tiempo. En los patrones se especula acerca de la posible relación entre eventos, lo cual lleva a analizar las

variables involucradas en los eventos en el tiempo. Cuando se llega al nivel de patrones se puede anticipar, planear y pronosticar.

Estructuras: relaciones circulares de causa-efecto que soportan y crean los patrones observables en los eventos. A este nivel puede llegarse a soluciones más robustas.

Modelos mentales: pensamientos o razonamientos existentes que permiten que la estructura sea como lo es, y se comporte como lo hace. Están compuestos por actitudes, creencias, expectativas, valores y experiencias. El nivel de modelos mentales permite crear soluciones que antes no existían, pero suelen ser difíciles de implementar. (Huigens, 2005).

Por último, resulta relevante mencionar que el enfoque de la dinámica de sistemas hace parte de los tres enfoques que existen actualmente para modelar el riesgo operacional teniendo en cuenta los datos históricos y el aporte de los expertos. Estos enfoques son:

1. **Dinámica de sistemas**: desarrolla un mapa sistémico de relaciones de causa – efecto, cuantificando cada relación a partir de la combinación de datos y conocimiento de expertos. Esta también busca reflejar explícitamente la incertidumbre como rangos alrededor de puntos estimados. El resultado de este método es la simulación de los rangos de salidas y el resumen de estos rangos como distribuciones de probabilidad. (Shah, 2001)

2. **Redes Bayesianas (BBN):** este método está basado en la regla de Bayes desarrollada por Thomas Bayes (1763), el cual es usado principalmente en la toma de decisiones. Las redes bayesianas están compuestas por nodos que representan las variables de decisión, las variables causales y las variables de salida. Los arcos que conectan los nodos indican la relación lógica causal, y los nodos de probabilidad indican las probabilidades de los diferentes valores que puede tomar una variable en un nodo. Esta técnica tiene similitud con la dinámica de sistemas, sin embargo, esta última ofrece una mayor flexibilidad a la hora de modelar. (Shah, 2001)

3. **Lógica borrosa:** está basado en la teoría desarrollada por Lotfi Zadeh y su aplicación principal se da en los sistemas de control de ingeniería, razonamiento cognitivo e inteligencia artificial. En este método se establecen unos conjuntos borrosos, donde para elemento del conjunto, se determina un indicador de grado de verdad para analizar la relevancia del elemento en dicho conjunto. Este grado de verdad puede tomar valores entre el 0% y el 100%, donde un mayor valor de este indicador señala una mayor importancia del individuo. En los conjuntos borrosos se utilizan variables lingüísticas en lugar de variables numéricas. Adicionalmente se establecen reglas borrosas, las cuales son especificadas por expertos, para definir relaciones de causa y efecto. (Shah, 2001)

2. PROCEDIMIENTO O DISEÑO METODOLOGICO

Con el fin de cumplir el objetivo general de plantear un modelo de gestión de riesgo operativo con un enfoque sistémico, se eligió una metodología que integra varias teorías y métodos que apuntan a cumplir cada uno de los objetivos específicos estipulados para el cumplimiento del primero. El marco metodológico general se basa en la Teoría del Icerberg de Daniel Kim, explicada en el marco teórico. Allí se propone que para llegar al nivel de estructuras, que es el foco de interés, se debe comprender primero el nivel de eventos y patrones. En este orden de ideas, los pasos a seguir se describen a continuación:

2.1 SIMULACIÓN DE DATOS DE PÉRDIDAS (NIVEL DE EVENTOS).

Se van a simular datos de pérdida para el tipo de evento de riesgo operacional de fraude externo, específicamente la categoría de seguridad de los sistemas. En esta categoría se consideran los daños por ataques informáticos y el robo de la información con pérdidas monetarias.

Se simularán los datos teniendo en cuenta que estos eventos pueden simularse mediante distribuciones de probabilidad discretas para las frecuencias de los eventos y continuas para la severidad de los mismos. En la generación de los datos se buscará lograr una media alta que incluya valores de severidad altos y bajos, que permita establecer un umbral alto. Además, para definir las distribuciones de probabilidad adecuadas se analizarán distintos estudios a nivel internacional sobre cuantificación del riesgo operativo con el enfoque de la distribución de pérdidas.

La distribución de pérdidas usualmente se hace para un conjunto de eventos de una línea de negocio asociados a un tipo particular de riesgo (Peña, Bonet, & Lochmuller, 2018), por esto se simularán los datos para una sola categoría de riesgo operacional. Además, porque lo que se busca es proponer un modelo de gestión que posteriormente pueda ser utilizado con datos reales de entidades y que sirva de base para el desarrollo de los modelos de gestión de los demás tipos de riegos operativos.

Así, inicialmente se realizó una búsqueda bibliográfica que permitiera establecer las distribuciones de probabilidad que comúnmente definen la frecuencia y la severidad de los eventos de riesgo operacional. Mora (2009) expone que para simular la frecuencia de los eventos de pérdida operacional deben utilizarse distribuciones discretas tales como *Poisson* o Binomial Negativa, mientras que para la severidad de los mismos sugiere distribuciones continuas de cola larga como la distribución *Lognormal*, *Weibull* y generalizada de Pareto.

Fontnouvelle et al. (2003) en un estudio de la Reserva Federal del Banco de Boston para cuantificar el riesgo operacional a partir de datos de pérdidas, utilizaron datos de dos consorcios: OpRisk Analytics y OpVentage. Es importante mencionar que los datos que son entregados por los consorcios usualmente son recolectados de fuentes públicas como reportes de periódicos, presentaciones de la Corte y reportes de la Comisión de Bolsa de

Valores de Estados Unidos; y que estas bases de datos proporcionadas incluyen la clasificación de pérdidas por línea de negocio y tipo de evento.

A partir de estos datos, los investigadores realizaron un procedimiento estadístico con el fin de disminuir el sesgo presente en los datos debido a que normalmente en las fuentes públicas solo se reportan eventos de severidad alta. Finalmente, para obtener la distribución de pérdidas de riesgo operacional hacen uso de la distribución de *Poisson* con un parámetro de lambda entre 30 y 100 para la frecuencia, y una distribución de severidad *Logexponencial.* (de Fontnouvelle, De Jesus-Rueff, Jordan, & Rosengren, 2003)

Con este estudio se evidencia que trabajar con datos de consorcios no resulta ser adecuado debido al sesgo residual que queda en la data una vez aplicado el procedimiento estadístico. Además, las bases de datos de consorcios recopilan eventos de pérdidas principalmente de entidades de Estados Unidos, y para tener acceso a esta información debe establecerse una relación contractual o de inscripción paga con el consorcio. (de Fontnouvelle, De Jesus-Rueff, Jordan, & Rosengren, 2003)

Otros estudios como el de Otero & Venerio (2009) y el Franco & Murillo (2008) también sugieren que las distribuciones más recomendables a la hora de modelar la severidad son la *Lognormal* y *Weibull,* y para la frecuencia *Poisson*, *Binomial* o *Binomial Negativa*. Sin embargo, los segundos autores apuntan que en la práctica ninguna distribución simple se ajusta a los datos de severidad satisfactoriamente, por lo que es necesario recurrir a una mixtura de distribuciones.

Complementando lo anterior, Andrés Mora Valencia (2010) en un estudio realizado afirma que diferentes autores ajustan las distribuciones de severidad paramétrica a los datos de pérdida para estimar los parámetros de la distribución y medidas de riesgo. También menciona que, para modelar la frecuencia de las pérdidas por riesgo operativo, los autores consideraron la distribución de Poisson y la distribución binomial negativa.

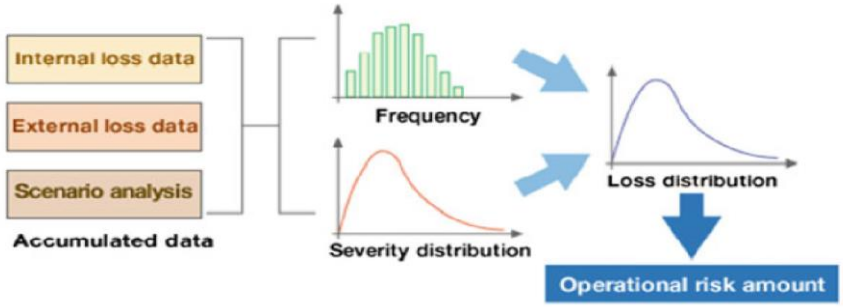
Asimismo, Arbeláez & Murillo (2008) proponen la distribución de Poisson como una candidata con muchas ventajas a la hora de modelar la frecuencia de los datos, sin embargo, recomiendan contemplar otras alternativas como la binomial o la binomial negativa. Por otra parte, proponen la distribución Lognormal o la de Weibull a la hora de modelar la severidad, aunque mencionan que en la práctica ninguna distribución simple se ajusta a los datos satisfactoriamente; de ahí la necesidad de recurrir a una mixtura de distribuciones para variables aleatorias continuas.

Teniendo en cuenta los resultados anteriores, se eligió simular la frecuencia de los eventos de pérdidas a partir de una distribución de *Poisson* y la severidad a partir de la distribución *Lognormal.* Se eligieron estas distribuciones debido a que éstas son las distribuciones que según la literatura ofrecen un mejor ajuste de los datos de frecuencia y severidad en la cuantificación del riesgo. No obstante, teniendo en cuenta que en la práctica ninguna distribución simple se ajusta adecuadamente a los datos de severidad, es importante mencionar que, al simular los datos de severidad a partir de la distribución Lognormal, este supuesto puede llevar a una sub-valoración del OpVar en el desarrollo del trabajo.

2.2 APLICACIÓN DEL ENFOQUE DE LA DISTRIBUCIÓN DE PÉRDIDAS-LDA (NIVEL DE PATRONES)

A partir de los eventos del riesgo operativo simulado, se construyó un prototipo del modelo causal en la herramienta IThink para generar los datos de frecuencia y severidad del tipo de riesgo simulado con el fin de observar el patrón de comportamiento de los datos, y los eventos de riesgo de mayor ocurrencia. Este análisis es importante para poder establecer posteriormente los diferentes escenarios que permitirán realizar el comparativo entre las magnitudes del capital regulatorio que varían desde el modelo causal en función de la gestión del riesgo.

Ilustración 2. Distribución de Pérdidas



Fuente: (Chaudhuri & Ghosh, 2016)

Inicialmente para la simulación del modelo se eligieron los parámetros que se observan en la siguiente tabla tomando como marco de referencia los valores encontrados en los estudios mencionados en el apartado anterior, además se decidió partir de valores bajos para simular un escenario optimista donde la empresa no experimenta gran frecuencia de ataques exitosos y que la severidad de los eventos de riesgo es baja.

Tabla 4. Parámetros

Distribución	Parámetros	Valor
Poisson	λ	7.5
Lognormal	μ,σ	10,2.5

Fuente: elaboración propia.

Además como parámetros de la simulación, también se estableció en que el modelo causal se iba simular en una unidad de tiempo mensual y a analizar por periodos de 12 meses puesto que en realidad el capital regulatorio debe calcularse para cada año.

Con los dos pasos anteriores se abarca el nivel de eventos y de patrones de la teoría del Iceberg, dando paso así al siguiente nivel que es el de estructuras. Para el siguiente nivel

se utiliza la información sobre los eventos y frecuencias analizada en este primer paso para la formulación del sistema de estudio.

2.3 APLICACIÓN DE LA TEORÍA GENERAL DE SISTEMAS (NIVEL DE ESTRUCTURAS)

A partir de la aplicación de esta teoría se pretende abarcar los dos últimos objetivos específicos, esta se divide en dos fases e incorpora herramientas del enfoque holístico que permiten ejecutar las fases propuestas.

Así, para el desarrollo de esta sección de la metodología se tomará como base el estudio realizado por Derek L. Nazareth y Jae Choi citado en el apartado de antecedentes, puesto que estos autores desarrollan un modelo de dinámica de sistemas para la administración de la seguridad de la información. Lo anterior implica que en este estudio se identificaron adecuadamente las variables que interfieren en la administración de la seguridad de la información, y como el tipo de riesgo que se desea estudiar es la seguridad de los sistemas, resulta pertinente tomar como referencia el estudio realizado por estos autores para desarrollar el modelo propio.

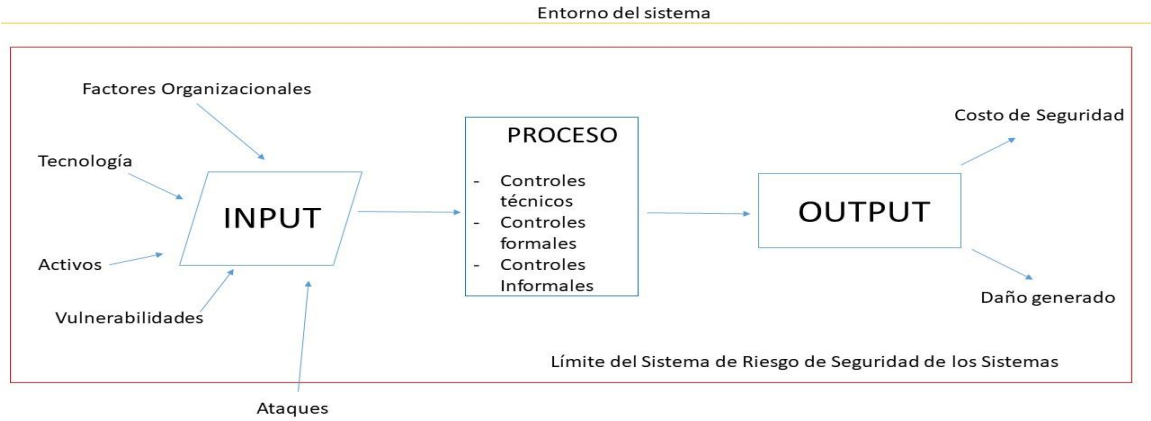
El modelo base se modificará tanto en estructura como en las ecuaciones que describen el comportamiento de las variables, con el fin de incorporar los elementos referentes a la frecuencia de los eventos de riesgo y la severidad para cada uno de ellos, con el fin de poder acumular la información para un período de 12 meses. Finalmente, se pretende calcular el valor en riesgo operacional teniendo en cuenta la gestión de las demás variables.

FASE I

a. Conceptualización del modelo y de su entorno

A partir de las variables que intervienen en los eventos de riesgo se debe delimitar el sistema de estudio, además de identificar los flujos de entrada, proceso y salida del sistema. Se espera que el sistema de estudio incluya personas, tareas, documentación, software, organización, pues este tipo de variables son las pertenecientes al riesgo operativo. Con el fin de facilitar esta etapa, a continuación, se presenta un diagrama con la descripción general del sistema que rodea al riesgo objeto de estudio. En este se definió el entorno del sistema y los límites del mismo; dentro de los límites del sistema se encuentran las entradas, los procesos internos y las salidas que hacen parte del riesgo de la seguridad de los sistemas.

Ilustración 3. Caracterización del sistema del riesgo de Seguridad en los sistemas



Fuente: elaboración propia.

Posterior a la construcción del diagrama, se establecieron los aspectos relacionados a cada uno de los elementos allí expuestos con el fin de definir todas las variables que serán tenidas en cuenta en el modelo.

Entradas

- Factores organizacionales: imagen corporativa, valor percibido del target, atractivo del target.
- Tecnología: inversión en seguridad, debilidades base de los sistemas, debilidades desarrolladas del sistema, procedimientos de seguridad, riesgo de seguridad del software
- Activos: inversión acumulada en herramientas de seguridad, inversión acumulada en disuasión, valor del activo.
- Vulnerabilidades: vulnerabilidad acumulada, vulnerabilidad percibida, vulnerabilidad del sistema, esfuerzo de reducción de vulnerabilidad.
- Ataques: motivación de ataque, disponibilidad de herramientas de ataque, número de atacadores, número de ataques, probabilidad de ataque.

Proceso

- Controles técnicos: inversión en herramientas de seguridad, inversión en seguridad.
- Controles formales: habilidad de detección, esfuerzo de recuperación, ataques reportados, esfuerzo de evaluación del riesgo, procedimientos de seguridad.
- Controles informales: inversión en disuasión, impacto de disuasión.

Salidas

- Costo de seguridad: costo acumulado de seguridad, costo de seguridad.
- Daño generado: daño, total de ataques, inmediatez del daño, magnitud del daño, ataques prevenidos, ataques exitosos.

En general, el modelo estará conformado por tres tipos de variables: continuas, discretas y variables continuas que describen probabilidades. El valor del activo, la magnitud del daño, la inversión en disuasión y la inversión en seguridad son variables continuas en unidades monetarias (dólares), por otra parte, el número de ataques, número de ataques prevenidos y número de ataques exitosos son eventos discretos que tendrán una frecuencia específica determinada por el modelo. Las demás variables son proporciones o probabilidades.

Es importante mencionar que las ecuaciones utilizadas para determinar el valor de las proporciones están basadas en el modelo de referencia. Estas fueron adaptadas al modelo específico de gestión aquí propuesto teniendo en cuenta además que todas las proporciones y probabilidades deben estar en un rango entre 0 y 1. También se procuró utilizar valores medios para algunas proporciones puesto que como se ha dicho, lo que se pretende es obtener un modelo generalizado.

b. Construcción del modelo

En esta etapa se busca establecer las relaciones causales entre los elementos identificados en la etapa anterior mediante el modelo de sistémica holístico, presentado a continuación, y diagramas de bucles causales. Posterior a la construcción de los bucles causales, se formará el sistema dinámico mediante la unión causal de los diferentes bucles individuales.

Ilustración 4. Modelo Sistémico-Holístico

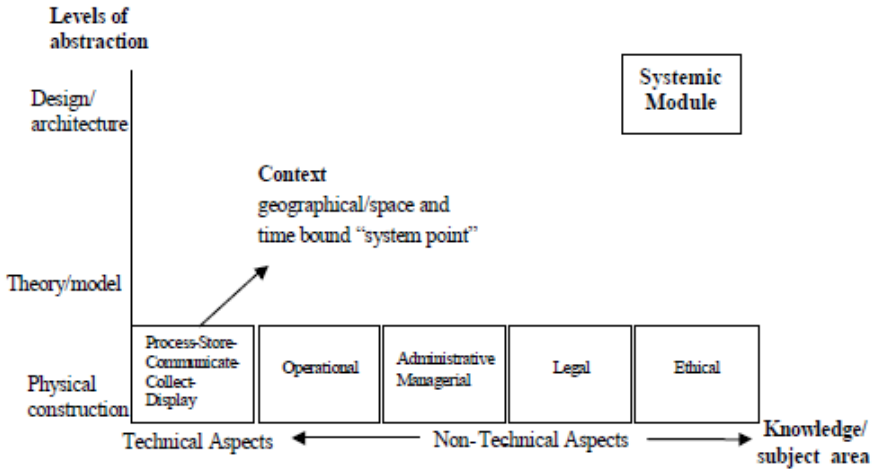


Figure 2.5.1: Details of the Framework and the Methodology for Security Informatics – the Systemic-Holistic Model [125]

Fuente: (Kessler, A Sytemic Approach Framework for Operational Risk, 2007)

Para la construcción del modelo causal se utilizó el diagrama descrito en el apartado anterior y el modelo base, los cuales abarcan las variables anteriormente. El modelo construido es un modelo de gestión puesto que supone una compresión de los aspectos dinámicos de todas aquellas variables donde la gerencia de una entidad puede intervenir por medio de decisiones estratégicas. Algunas de estas variables son la inversión en seguridad, la inversión en herramientas de disuasión, esfuerzos de prevención y recuperación.

Previo a la descripción de las variables del modelo es importante explicar las notaciones propias del programa de modelación utilizado para su construcción. En el modelo los rectángulos representan stocks que pueden acumular valores a través del tiempo, estos stocks son influenciados por flujos, los cuales son representados por medio de una flecha doble y un símbolo de válvula. Estos últimos se definen por medio de ecuaciones que alimentan los valores de los stocks.

En el modelo también se encuentran los convertidores, los cuales se representan mediante círculos. Algunos de ellos están determinados por valores estáticos y otros por ecuaciones que incluyen las variables con las cuales el convertidor esté relacionado mediante conectores. Por último, los conectores poseen un signo negativo o positivo para indicar si el incremento en una variable conlleva a un incremento o decremento en otra. De igual forma, los signos permiten caracterizar los bucles que se forman dentro del modelo, siendo los bucles de refuerzo aquellos que tienen todas las conexiones con signos positivos, y los bucles de balance aquellos que tienen al menos un signo negativo.

Para describir el modelo causal se partió del hecho de que la inversión que se realiza para prevenir los ataques relacionados con el riesgo de seguridad en los sistemas, está relacionada directamente con los ataques y posibles amenazas informáticas. Lo anterior debido a que, si existe una mayor inversión para prevenir los eventos de riesgo, la tasa de ataques o amenazas será menor.

De manera general el modelo está construido a un nivel organizacional y bajo una perspectiva económica puesto que lo que se quiere observar es cómo la gestión de las variables que interfieren en el riesgo de seguridad de los sistemas impacta en la cuantificación del valor en riesgo operacional. El modelo está compuesto por los siguientes segmentos: ataques, riesgo del software, recuperación, vulnerabilidad y consideraciones económicas.

En primera medida se identificó que la *imagen corporativa* de la organización combinada con su *valor percibido* condiciona el atractivo de la misma como blanco para ataques externos. Es por esto que en el modelo se define el *atractivo del target* como una función de las dos variables anteriores, y en consecuencia estas tres variables se encuentran conectadas en el modelo.

El *atractivo del target* influencia a su vez a la *probabilidad de ataque,* la cual también se ve influenciada por la *motivación* interna de los atacadores, la *vulnerabilidad percibida* de los sistemas de la entidad y las actividades de *disuasión.* Todas las variables anteriores generan un incremento en la *probabilidad de ataque* excepto la *disuasión* puesto que las actividades de disuasión hacen referencia a las políticas y procedimientos internos relacionados con el cumplimiento de los empleados para evitar nuevos eventos de ataques, y las actuaciones frente a los atacadores ya identificados.

Para definir las ecuaciones que describen las anteriores variables se tuvo en cuenta que la *vulnerabilidad percibida*, *el atractivo del target* y la *motivación* tienen un efecto cada vez mayor en la *probabilidad de ataque*, aunque a un ritmo decreciente. Por tanto, son modeladas por medio de una aproximación de una función exponencial negativa. Por su parte, el impacto de la disuasión al tener una relación inversa con la *probabilidad*, es modelada con una función convexa decreciente. Finalmente, la ecuación de *la probabilidad de ataque* fue validada con diferentes pruebas para asegurar que los efectos acumuladores de las otras variables permitan una probabilidad en un rango entre 0-1.

Después de definir la *probabilidad de ataque,* se consideró el primer segmento del modelo mencionado que es el de ataques. El *número de ataques* que la entidad puede enfrentar se definió con base en la *probabilidad de ataque, el número de posibles atacadores* externos y la *disponibilidad de los instrumentos* para realizar los ataques. Del número de ataques totales se desprenden dos variables más: *ataques prevenidos* y *ataques exitosos*. Los *ataques prevenidos* están influenciados por la *habilidad de detección* de la entidad, que a su vez depende de la *inversión en herramientas de seguridad* que esta posea. Los *ataques exitosos* se definen como el número de *ataques totales* multiplicado por la proporción restante a la habilidad de detección (1-Habilidad de Detección). De todas las variables mencionadas hasta el momento, el número de *ataques exitosos* será una de las salidas de

mayor importancia puesto que los resultados de esta variable serán las frecuencias mensuales de los eventos de riesgo.

Como se mencionó anteriormente, la *habilidad de detección* de una entidad se ve influenciada por la inversión que esta haga en herramientas de seguridad. Para definir esta variable se tuvo en cuenta que la *inversión en seguridad* no es necesariamente continúa debido a que una inversión cada cierto tiempo permite a la compañía detectar los ataques. Es por esto que la *inversión en herramientas de seguridad* se definió cada 6 meses. Así, la *inversión acumulada en herramientas de seguridad* se define como un acumulador de dicha inversión realizada cada 6 meses. Teniendo en cuenta lo anterior, la *habilidad de detección* se modela como una función exponencial negativa puesto que esta variable va a aumentar con una mayor *inversión en herramientas de seguridad,* pero cada vez a una menor tasa.

Mientras que el *número de ataques prevenidos* está determinado por el aumento en la *habilidad de detección*, el número de *ataques exitosos* genera diferentes efectos. El daño causado por los ataques exitosos es capturado a partir de dos dimensiones: la magnitud del daño, y la urgencia de recuperarse del daño causado (*urgencia de recuperación*). Asimismo, los ataques exitosos van a generar publicidad, dicha publicidad es representada por medio de los *ataques reportados* capturados por el modelo. Estos informes incluyen la no disponibilidad del sitio, la falta de disponibilidad de los activos, el reconocimiento público de los ataques exitosos y los informes presentados a las agencias gubernamentales para fines de cumplimiento. Es importante mencionar que algunos stocks, como el de *ataques prevenidos* y el de *costos de seguridad acumulada*, fueron incluidos en el modelo únicamente para acumular valores durante la simulación, por lo cual no son determinados por otras variables del mismo.

En cuanto a la *magnitud del daño*, la *inmediatez del daño* y el *número de los ataques exitosos*, estas son variables que van a ayudar a determinar el alcance de los informes de ataque, donde aquellos que sean compartidos por medios publicitarios van a determinar la vulnerabilidad percibida de los activos de la información de la organización. La relación entre estas variables caracteriza un bucle de refuerzo, el cual indica que los ataques exitosos darán lugar a más ataques y que la prevención efectiva de los ataques hará que los atacantes busquen otros objetivos más fáciles o más atractivos.

La *inmediatez del daño* se ve influenciada por los *ataques exitosos*, y esta a su vez influencia positivamente los *ataques reportados* y *el esfuerzo de evaluación de los riesgos*. Asimismo, *la magnitud del daño*, además de incidir directamente en el esfuerzo de *recuperación* y *los ataques reportados*, también afecta de forma creciente y directa el *esfuerzo de evaluación de los riesgos*, el cual no pretende hacer una reevaluación completa del sistema para identificar las vulnerabilidades nuevas, sino que busca hacer una evaluación incremental del sistema. Algunas actividades que se pueden implementar para reducir estos riesgos son la aplicación de fortalecimientos al Software, actualización del Software y realizar cambios en los procedimientos de acceso, y seguridad de los sistemas. Por otro lado, la *magnitud del daño* aumenta en razón del *valor del activo* y los *ataques exitosos*.

Otro segmento del modelo aborda la recuperación, las vulnerabilidades del sistema y el riesgo residual que se puede presentar en el mismo, esto teniendo en cuenta que el *daño* que ocasiona un *ataque exitoso* hará que se inicie inmediatamente un esfuerzo de recuperación donde entre mayor sea el daño, mayor va a ser el *esfuerzo de recuperación* del sistema y por ende el *costo de seguridad* también va a aumentar. Hay que tener en cuenta que, dependiendo de la naturaleza y el alcance del daño, el esfuerzo de recuperación puede ser simple o complejo dependiendo de la cantidad de tiempo que tarde dicha recuperación. Por ejemplo, restaurar datos de una copia de seguridad implica una recuperación simple, mientras que la reconstrucción de varios servidores, incluidos el software y hardware, implica una reconstrucción compleja.

Como se indica en el modelo, las vulnerabilidades del sistema están inversamente relacionadas con el *esfuerzo de reducción de vulnerabilidad*, con lo cual se espera que las vulnerabilidades disminuyan con mayores niveles de esfuerzo de reducción de vulnerabilidad. La *vulnerabilidad del sistema* se determina con los procedimientos de seguridad y el riesgo de seguridad del software, a medida que se implementen procedimientos de seguridad más efectivos, disminuye la vulnerabilidad del software. Por su parte, el *riesgo de seguridad del software* tiene un impacto directo sobre la vulnerabilidad del sistema ya que sobre esta variable inciden de forma positiva los *defectos base del software* y *el desarrollo de fallas en el software*. Sin embargo, estas últimas disminuyen ante un mayor esfuerzo de reducción de vulnerabilidad. Así, las vulnerabilidades en la base y el desarrollo del software, combinados con la solidez de los procedimientos de seguridad, determinarán la *vulnerabilidad general del sistema*.

Los informes acumulados de vulnerabilidad del sistema estructurarán la *vulnerabilidad percibida* por los atacantes ya que esta última variable se ve afectada negativamente no solo por estos informes, sino también por los informes de ataque realizados. Es importante aclarar que, aunque se pueden tomar medidas para eliminar algunas vulnerabilidades, estas no afectarán la vulnerabilidad percibida a menos que se publiquen. Además de lo ya mencionado, *la vulnerabilidad percibida aumentará la probabilidad de ataque*, lo cual completa un segundo bucle en el modelo.

En la probabilidad de ataque inciden directamente la motivación de ataque y el atractivo del objetivo, como se explicó el inicio de la descripción del modelo. Po su parte, el impacto de disuasión, el cual incide de forma inversa sobre la probabilidad de ataque, aumenta con una mayor inversión en seguridad.

La parte final del modelo se relaciona con la inversión y los costos de seguridad, ya que las organizaciones invierten en acciones disuasivas y herramientas de seguridad para detectar y prevenir ataques como se ha mencionado anteriormente. La inversión acumulada en herramientas de seguridad determina la capacidad de detectar y detener ataques. De forma similar, la inversión de disuasión acumulativa configura el impacto disuasorio, que en sí forma parte del ciclo de ataque.

Las inversiones en herramientas de seguridad y disuasión representan costos para la organización y, combinados con el esfuerzo de reducción de vulnerabilidad, constituyen la inversión de seguridad para la organización. Los costos de evaluación de riesgos y los

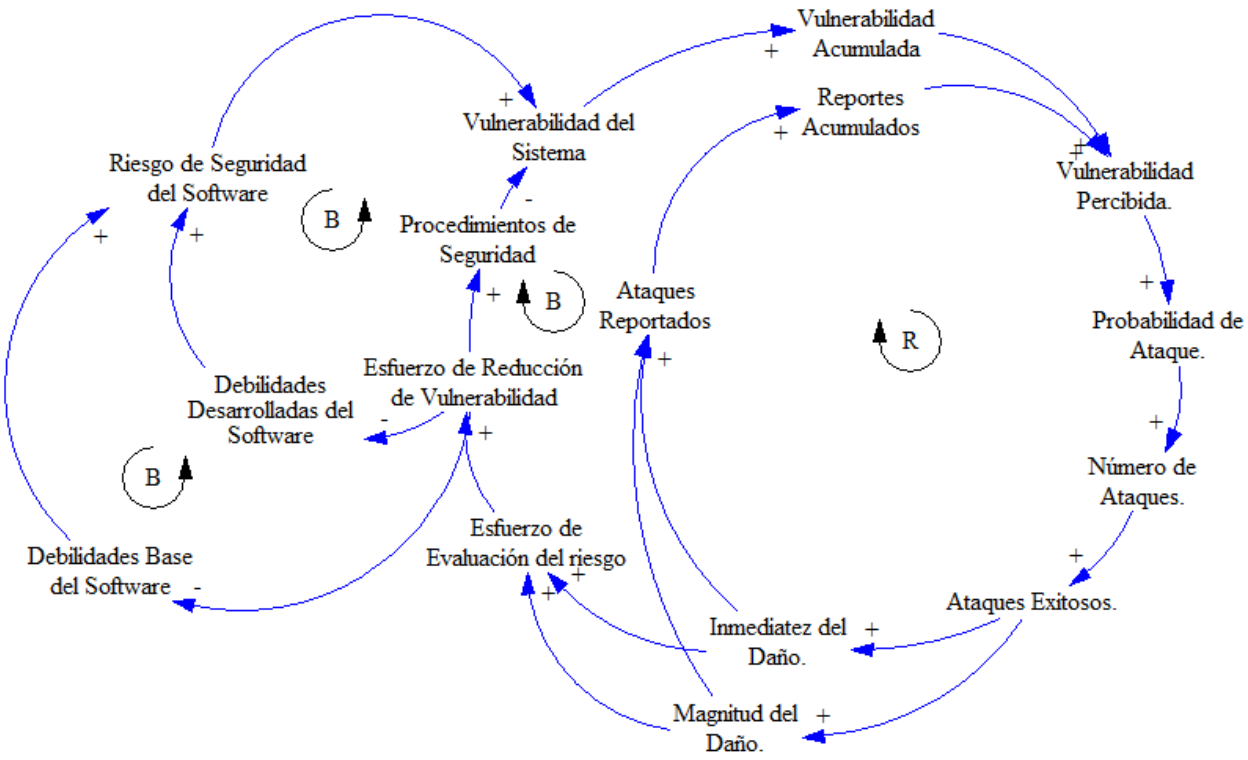
costos de recuperación contribuyen aún más al costo general de seguridad de la empresa. Para mayor practicidad, se utiliza una acción para calcular el gasto de seguridad total en el transcurso de la simulación.

El modelo de manera total incluye un bucle de refuerzo y tres bucles de equilibrio. El primero se centra en los ataques de seguridad, donde los ataques exitosos generan publicidad con respecto a la vulnerabilidad percibida, atrayendo así a más atacantes. Este comportamiento continuará sin disminuir, pero se mantiene bajo control mediante los bucles de equilibrio que involucran vulnerabilidades del sistema. La detección de ataques exitosos conduce a una variedad de actividades de reducción de vulnerabilidad, que incluyen el arreglo de fallas de software básicas, la eliminación de fallas de software desarrolladas y la implementación de nuevos procedimientos de seguridad. Lo anterior se puede evidenciar en el diagrama de bucles causales (ver Ilustración 5).

Una vez definido todo el diagrama causal del riesgo en estudio, se estableció que las variables de salida del modelo serían el número de ataques exitosos y la magnitud del daño de dichos ataques. El número de ataques exitosos representa la frecuencia del riesgo y la magnitud del daño, es decir, la severidad de los mismos. Con el propósito de capturar estas variables para su posterior utilización en la cuantificación del riesgo, se crearon dos stocks adicionales para acumular los valores de frecuencia y severidad de la simulación.

Así, luego de tener definido este diagrama, se procedió a construir el modelo de flujos y niveles (ver Anexo2).

Ilustración 5. Diagrama de Bucles Causales



Fuente: elaboración propia

c. Simulación del modelo construido.

Por medio del programa IThink, se simulará la estructura causal construida en el paso anterior, con el fin de verificar la interacción entre las variables e identificar aquellas con mayor influencia en el sistema. Además por medio de esta simulación se buscará obtener la frecuencia y severidad de los eventos, para luego construir la distribución de pérdidas (LDA).

d. Construcción de la distribución de pérdidas (LDA)

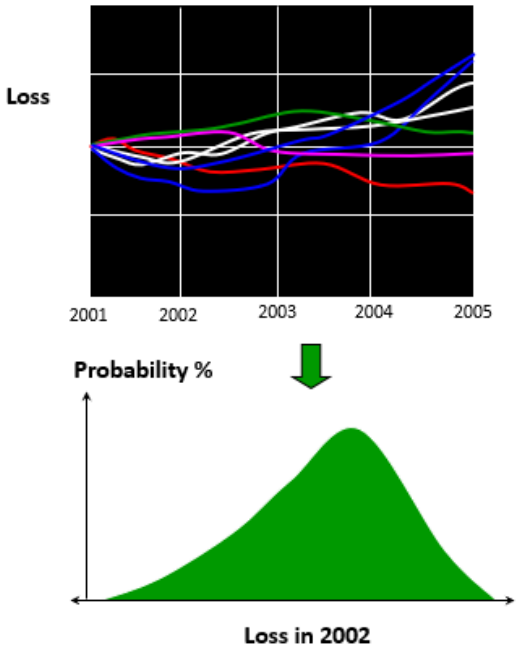
A partir de los datos arrojados por el modelo causal (frecuencia y severidad) se construirá la distribución de pérdidas que permite calcular el OpVaR.

FASE 2

a. Simulación de escenarios

El modelo dinámico se simulará con distintos escenarios con el fin de interpretar los patrones de riesgo a partir del modelo. Con base en los escenarios simulados se obtendrá la distribución total de pérdidas y se calculará el valor en riesgo OpVaR, el cual constituye el máximo valor en riesgo debido a eventos de riesgo operacional. Finalmente, se buscará proponer alternativas para disminuir el capital regulatorio teniendo en cuenta las variables de mayor influencia.

Ilustración 6. Análisis de escenarios



Fuente: (Shah, 2001)

2.4 PLANTEAMIENTO DEL MODELO FINAL Y RECOMENDACIONES

A partir de la simulación de escenarios se realizarán correcciones sobre el modelo dinámico, y se plantearán recomendaciones de control sobre las variables de mayor impacto en el riesgo operacional.

3. PRESENTACIÓN Y DISCUSIÓN DE RESULTADOS

3.1 DISTRIBUCIÓN DE PÉRDIDAS (LDA)

Como se estableció en el apartado de metodología, la primera etapa fue la simulación de un modelo inicial con el fin de validar la selección de las distribuciones de probabilidad. Una vez simulado el modelo inicial se ajustaron los datos generados a distribuciones de probabilidad con el fin de validar los supuestos establecidos inicialmente.

A continuación, se evidencia los resultados obtenidos:

Ilustración 7. Ajuste datos de frecuencia

Poisson	18.6 (2)	0.242	0.

detail

Poisson

lamda =	27.4545	
Chi Squared		
total classes		4
interval type		equal length
net bins		3
chi**2		18.6
degrees of freedom		2
alpha		5.e-002
chi**2(2,5.e-002)		5.99
p-value		9.01e-005
result		REJECT
Kolmogorov-Smirnov		
data points		22
ks stat		0.242
alpha		5.e-002
ks stat(22,5.e-002)		0.281
p-value		0.128
result		DO NOT REJECT
Anderson-Darling		
data points		0
ad stat		0.
alpha		5.e-002
ad stat(5.e-002)		0.
p-value		0.
result		DO NOT REJECT

En la ilustración 7 puede observarse que los datos de frecuencia generados por el modelo siguen una distribución de poisson según las pruebas Kolmogórov-Smirnov y Anderson Darling, para ambas pruebas el valor p es mayor al nivel de significancia de 5% y por tanto no puede rechazarse la hipótesis nula que sugiere una distribución de poisson para los

datos. No obstante, el parámetro lambda sugerido para los datos es de 27.45 y no 7.5 como indicaba el supuesto inicial.

Esta actividad permitió hacer ajustes en los parámetros del modelo y además verificar los supuestos de las distribuciones de probabilidad elegidas para la frecuencia y severidad. Sin embargo, cuando se validó la distribución de la severidad se encontró que para esta variable era necesario realizar varias iteraciones del modelo que generan distintas curvas de severidad, antes de ajustarla a una distribución de probabilidad específica. Teniendo en cuenta lo anterior, este procedimiento se realizó con el modelo causal final establecido para el escenario base.

3.2 ESCENARIO BASE

El escenario base se planteó para observar el comportamiento de una empresa pequeña, en este se utilizaron valores medianos para las construcciones sin dimensiones y un conjunto de valores ponderados para otras construcciones. Así, para el modelo se optó por tener un valor del activo por $5.000.000 y un número de atacadores igual a 100; además se determinó que la inversión en herramientas de seguridad iba a ser de $10.000 al inicio de cada año, con gastos en inversión de disuasión por $2.000 en el mismo período de tiempo. Luego de ejecutar el modelo, el análisis se concentró en el comportamiento del número de ataques exitosos, la magnitud del daño total y los costos de seguridad. Estos resultados se pueden observar a continuación.

Ilustración 8. Número de ataques

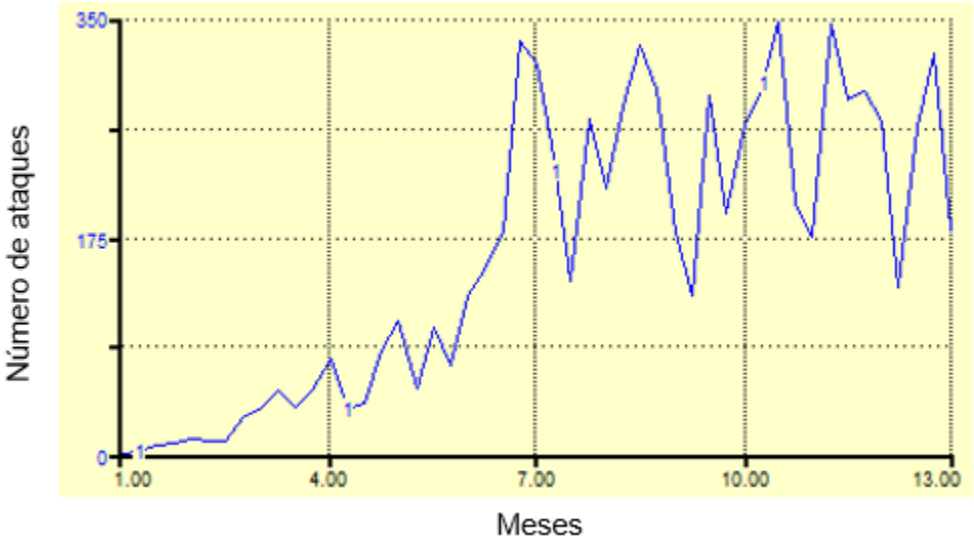


Ilustración 9. Magnitud del daño

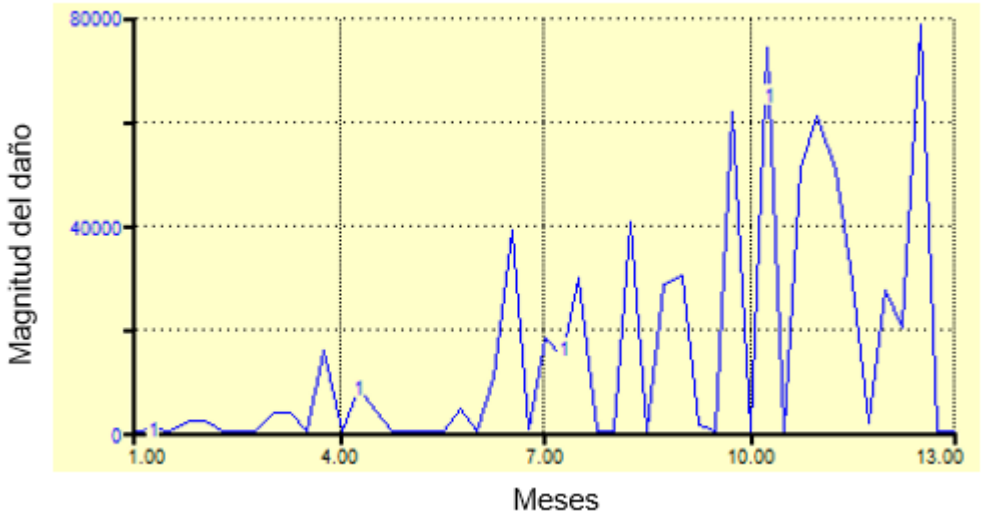
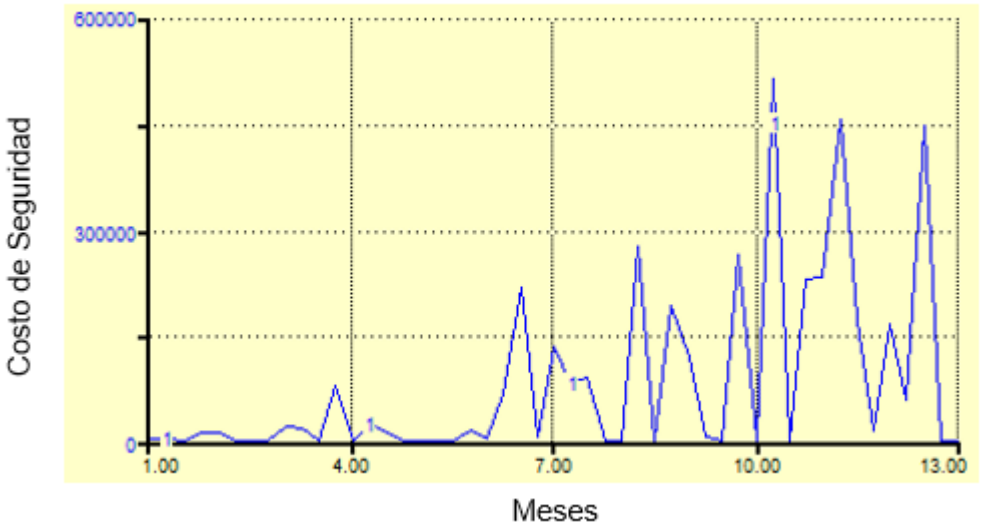


Ilustración 10. Costos de seguridad



Los datos mensuales encontrados en las variables observadas anteriormente tienden a ser irregulares; sin embargo, con el tiempo se puede observar una mejor imagen de las tendencias involucradas en cada una de estas. En cuanto al número de ataques (ver Ilustración 8), la gráfica correspondiente muestra una tendencia creciente con algunos retrasos en el patrón, lo cual indica que no todos los ataques son exitosos y por ende solo algunos de estos logran causar daño en el sistema de la organización. Las variaciones evidenciadas en la gráfica de número de ataques explican la variabilidad de la magnitud del

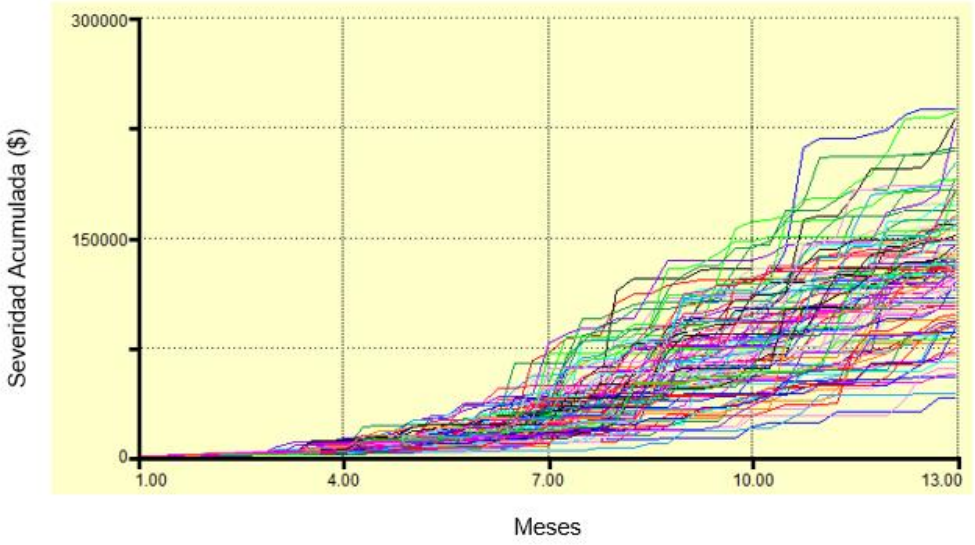
daño pues cualquier daño en los que se incurre por los ataques exitosos, desencadenan un esfuerzo de recuperación y por ende un esfuerzo de reducción de riesgo.

Respecto a los costos de seguridad (ver Ilustración 10), se puede observar que estos tienen un patrón de comportamiento similar al de la magnitud del daño (ver Ilustración 9), esto debido a que los costos de seguridad tienden a compensar los daños ocasionados por los ataques exitosos. En un esfuerzo adicional por validar el modelo, este fue sometido a un análisis de sensibilidad donde se cambiaron sistemáticamente los parámetros clave de entrada. No se observaron valores adversos, lo que sugiere que el modelo se estaba comportando satisfactoriamente.

Luego de comprobar que el modelo funcionaba correctamente, y teniendo en cuenta que es necesario obtener la distribución total de pérdidas para poder calcular el valor en riesgo OpVar, el modelo se corrió por un período de 1 año, cada 12 meses, con el fin de obtener el valor de la severidad acumulada al final del año. Se realizó la simulación del modelo 100 veces con el fin de capturar una cantidad de datos representativos que arrojaran una severidad acumulada objetiva. Es importante tener en cuenta que la severidad hace referencia a la magnitud del daño en el modelo.

En cuanto a la cantidad de simulaciones implementadas, es clave mencionar que solo se realizaron 100 simulaciones para la estimación del OpVar, por la capacidad de procesamiento de la máquina en la cual se realizó este procedimiento, no obstante, si se quiere tener mayor precisión en el cálculo de esta variable, se debe hacer un número de simulaciones del orden de mil o 10 mil como se plantea en la literatura, o utilizar un muestreo hipercubo latino que requiere menos iteraciones para cubrir todo el rango de la distribución. (Iman, Davenport, & Zeigler, 1980)

Ilustración 11. Severidad Acumulada



Al finalizar la simulación, se procedió a exportar los datos a un archivo de Excel con el fin de seleccionar únicamente los valores acumulados del último mes para poder construir con estos la distribución total de pérdidas en Stat Fit, y con esta hacer ajustes a los parámetros del modelo, además de verificar los supuestos de la distribución de probabilidad elegida para la severidad

Ilustración 12. Ajuste de Distribuciones

distribution	rank	acceptance
Erlang(-3.15e+004, 17., 9.64e+003)	100	do not reject
Gamma(-3.15e+004, 16.6, 9.88e+003)	91.5	do not reject
Beta(2.16e+003, 8.11e+005, 8.65, 45.1)	84.5	do not reject
LogLogistic(-3.28e+005, 20.9, 4.58e+005)	80.4	do not reject
Logistic(1.31e+005, 2.23e+004)	65.1	do not reject
Johnson SB(-1.02e+004, 3.45e+005, 0.731, 1.97	50.1	do not reject
Inverse Gaussian(-1.31e+005, 1.15e+007, 2.63	49.1	do not reject
Normal(1.32e+005, 4.e+004)	46.	do not reject
Weibull(3.13e+004, 2.68, 1.13e+005)	41.5	do not reject
Extreme Value IA(1.11e+005, 3.13e+004)	14.9	do not reject
Lognormal(2.34e+004, 11.5, 0.417)	13.8	do not reject
Triangular(3.86e+004, 2.53e+005, 1.13e+005)	12.6	do not reject

Ilustración 13. Ajuste Datos de Severidad Acumulada

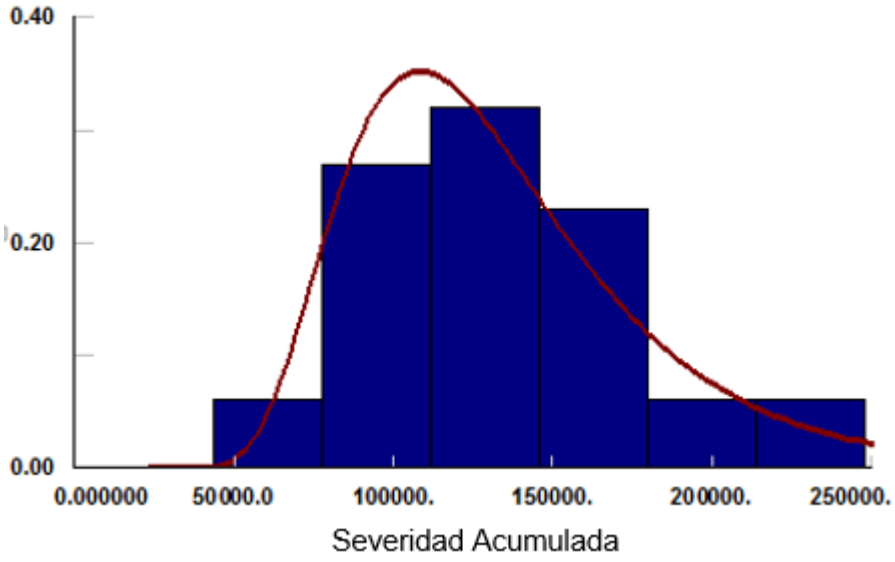
Lognormal			
minimum	=	23415.1	
mu	=	11.5214	
sigma	=	0.416536	
Kolmogorov-Smirnov			
data points			100
ks stat			9.4e-002
alpha			5.e-002
ks stat(100,5.e-002)			0.134
p-value			0.32
result			DO NOT REJECT
Anderson-Darling			
data points			100
ad stat			1.14
alpha			5.e-002
ad stat(5.e-002)			2.49
p-value			0.293
result			DO NOT REJECT

A pesar de que el programa Stat Fit sugería que los datos de severidad se podían ajustar a diferentes distribuciones (ver Ilustración 12), se decidió ajustar los mismos a la distribución Lognormal ya que en la revisión bibliográfica se encontró que diferentes autores concluían que la severidad se podía ajustar correctamente a esta distribución. De igual forma, con la Ilustración 14 se confirma que los datos si se ajustan adecuadamente a esta distribución.

En cuanto a la validación de los parámetros de la distribución seleccionada, puede observarse que los datos de severidad siguen una distribución Lognormal según las pruebas Kolmogórov-Smirnov y Anderson Darling (ver Ilustración 15). Para ambas pruebas el valor p es mayor al nivel de significancia de 5% y por tanto no se puede rechazar la hipótesis nula que sugiere una distribución lognormal para los datos. Sin embargo, los parámetros mu y sigma sugeridos para los datos son de 11.52 y 0.42 respectivamente, y no los valores de 10 y 2.5 como indicaba el supuesto inicial.

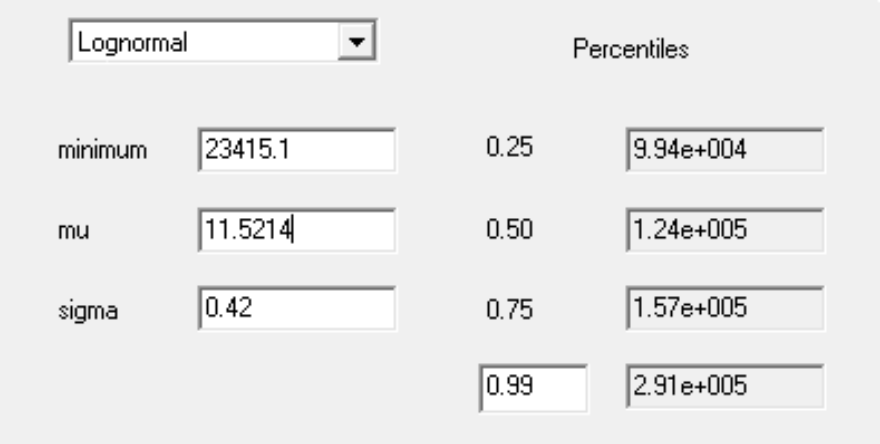
Cabe señalar que la prueba de Anderson Darling está diseñada para detectar discrepancias en las colas, y tiene una mayor potencia que la prueba de Kolmogorov-Smirnov. (Law, 2007)

Ilustración 14. Distribución Total de Pérdidas



Por último, teniendo en cuenta los parámetros arrojados por la distribución Lognormal, se calculó el OpVar con el percentil 99, el cual hace referencia al capital regulatorio que deben tener las empresas para soportar el riesgo operacional. Así, para este caso base se obtuvo que la empresa de análisis debe tener un capital regulatorio por valor de $291.000 dólares si esta realiza una inversión de seguridad de $10.000 y una inversión por gastos de disuasión de $2.000 durante cada año por un período total de 100 años.

Ilustración 15. Cálculo OpVar



3.3 ESCENARIOS ALTERNATIVOS DE INVERSIÓN EN SEGURIDAD

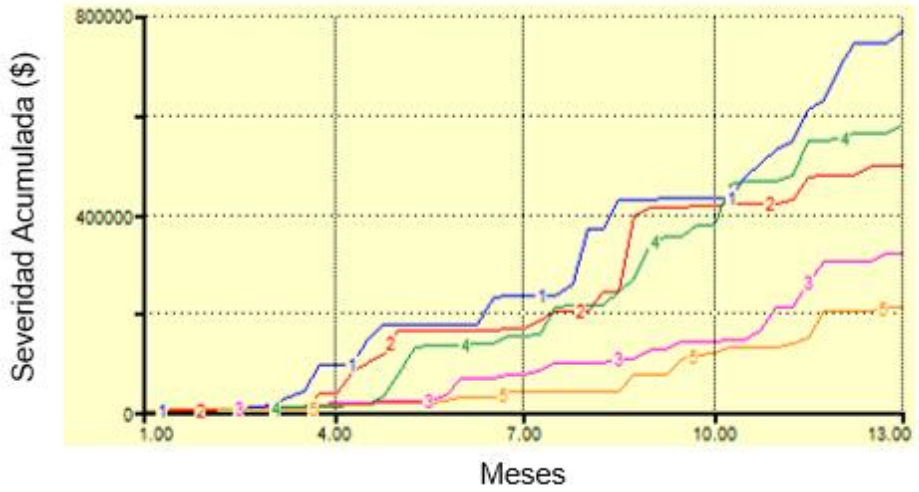
En el modelo planteado, la inversión en seguridad es una variable que depende únicamente de la compañía, esto debido a que es una variable de gestión y por ende la empresa es la que determina como se debe controlar. Así, se realizó un análisis de sensibilidad sobre esta variable para determinar cómo los cambios en la gestión de la misma afectan las demás variables consideradas en el modelo, además para analizar cómo los cambios en el monto de inversión en seguridad pueden afectar el valor total de capital regulatorio que debe tener la empresa para soportar el riesgo operacional.

Tomando como escenario base aquel donde la empresa realiza una inversión en seguridad de $10.000, se optó por realizar un análisis de sensibilidad partiendo de rangos de variación en seguridad, esto con el fin de determinar aquellos valores que implicarían un menor valor del OpVar en cada uno de los escenarios, y así por ende poder concluir acerca del valor en inversión de seguridad que le permitiría tener a la empresa un menor valor del capital regulatorio.

En primera medida se establecieron los rangos que se iban a implementar para el análisis, y posteriormente, para cada uno de los rangos determinados, se simuló el modelo 100 veces para identificar los valores de inversión que generarían los menores impactos en cada uno de estos. Lo anterior se realizó ya que las menores severidades generan como consecuencia un menor OpVar.

Rango 1: $3.000 - $7.000

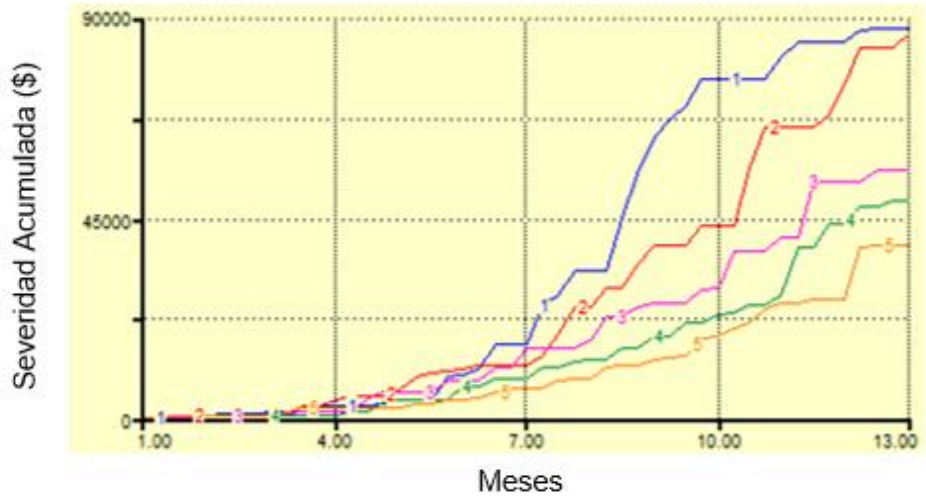
Ilustración 16. Escenario 1 Seguridad



En la gráfica anterior cada una de las curvas representa un valor diferente dentro del rango establecido, así la curva 1 representa una inversión de $3.000 mientras que la curva 5 representa una inversión de $7.000, esto teniendo en cuenta que cada curva tiene una diferencia de inversión de $1.000 respecto a la anterior. En la misma puede observarse claramente que la inversión de $7.000 es la que genera los menores valores de severidad acumulada.

Rango 2: $11.000 - $15.000

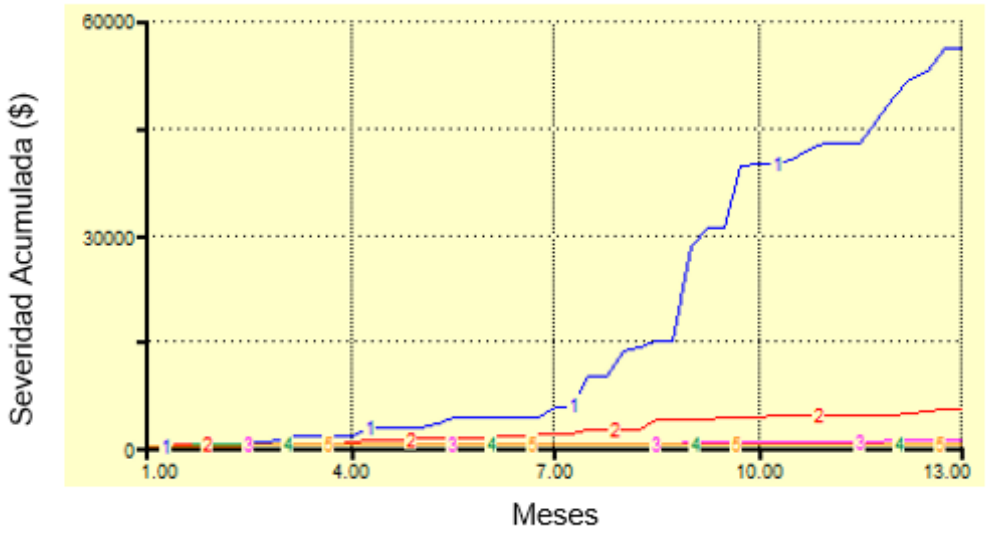
Ilustración 17. Escenario 2 Seguridad



En la gráfica, la curva 1 representa una inversión de $11.000 mientras que la curva 5 representa una inversión de $15.000. Según la misma puede concluirse que la inversión de $15.000 es la que genera las menores severidades en el modelo. Además, se puede observar que esta inversión de $15.000 ocasiona un nivel de severidad acumulada de aproximadamente $40.000, valor que es muy inferior a la severidad generada por la inversión en seguridad de $7.000 del rango anterior.

Rango 3: $15.000 - $55.000

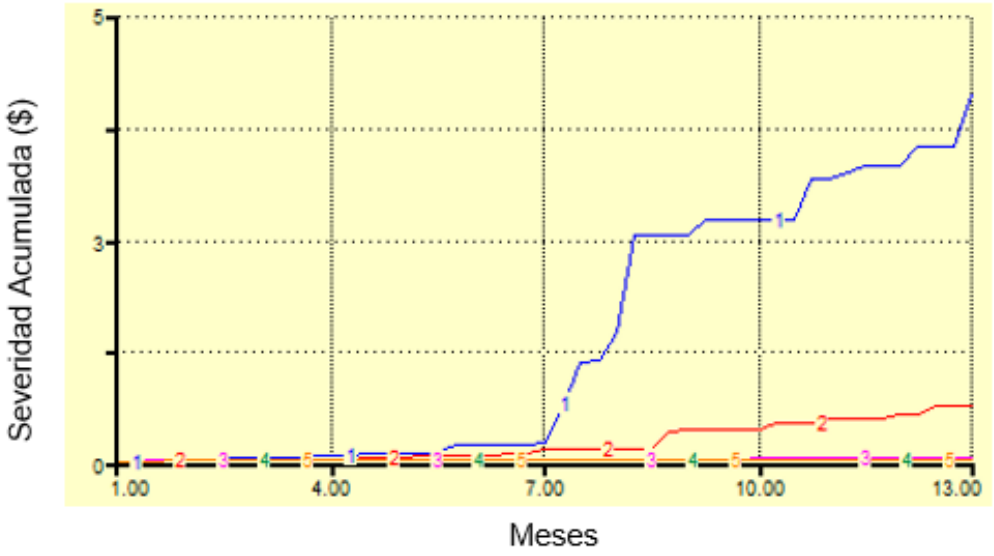
Ilustración 18. Escenario 3 Seguridad



En la gráfica, la curva 1 representa una inversión de $15.000 mientras que la curva 5 representa una inversión de $55.000. A partir de este rango se empezó a incrementar la inversión en $10.000, con el fin de poder determinar hasta qué valor era eficiente incrementar la inversión. Según la misma puede concluirse que la inversión de $55.000 es la que genera las menores severidades en el modelo, además de que se empieza a observar una tendencia donde a mayores niveles de inversión en seguridad, los valores de la severidad acumulada son menores, pues el valor de severidad generado por una inversión de $55.000 es inferior a los niveles óptimos encontrados en los rangos anteriores.

Rango 4: $60.000 - $100.000

Ilustración 19. Escenario 4 Seguridad



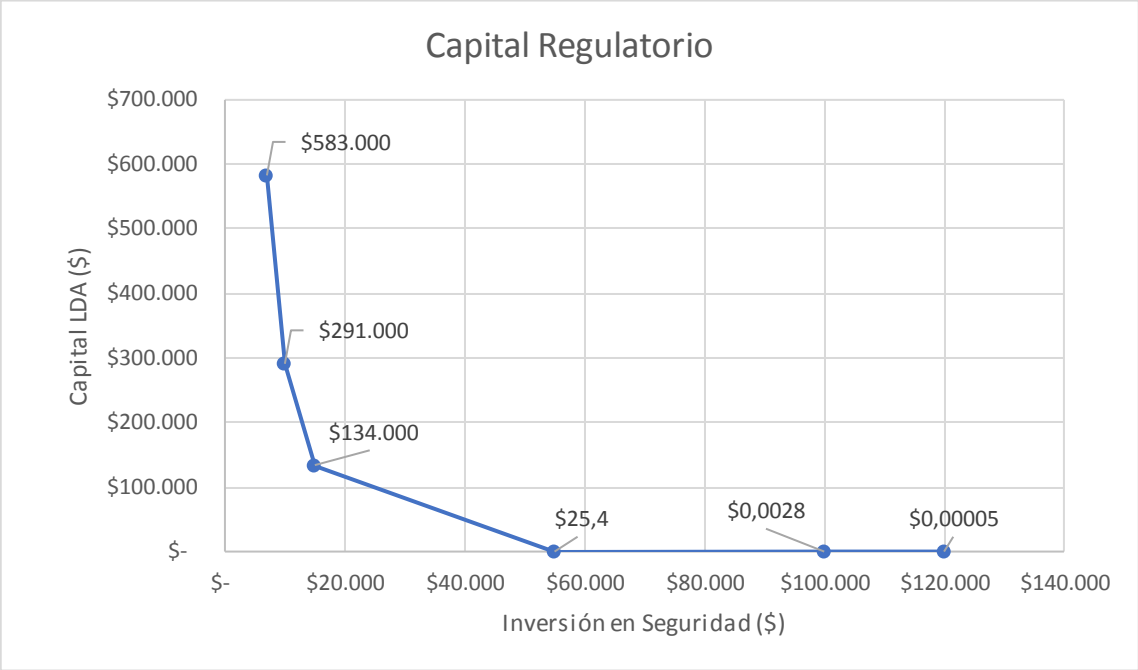
En la gráfica, la curva 1 representa una inversión de $60.000 mientras que la curva 5 representa una inversión de $100.000. Según la misma puede concluirse que la inversión de $100.000 es la que genera las menores severidades en el modelo, además de que se puede observar que la tendencia del rango anterior también se cumple en este escenario.

Una vez simulados todos los escenarios, se calculó el OpVar para cada uno de los valores de inversión en seguridad que generan los menores valores de severidad acumulada. Adicionalmente se calculó el capital regulatorio para una inversión de $120.000, esto con el fin de verificar el comportamiento decreciente de la LDA.

El análisis anterior generó como resultado que una inversión de $120.000 en herramientas de seguridad genera un OpVar de $5.09 x e-5 siendo este el menor valor de todos los escenarios. Esto implica que, con todas las demás variables de gestión constantes en el modelo, la empresa debe invertir esta cantidad de dinero en herramientas de seguridad para minimizar su capital regulatorio que soportará el riesgo operacional.

En la Ilustración 20 pueden observarse los diferentes valores OpVar para cada uno de los mejores escenarios de los rangos analizados. La curva de la gráfica demuestra que, con una mayor gestión, el capital regulatorio del riesgo operacional disminuye, por lo cual se puede concluir que estas dos variables son directamente proporcionales donde, si la empresa desea tener poca cantidad de dinero reservada para cubrir los eventos de riesgo, debe hacer un esfuerzo para invertir grandes sumas en seguridad.

Ilustración 20. Capital Regulatorio vs. Inversión en Seguridad



Finalmente se analizó el impacto de la inversión en seguridad en el número de ataques exitosos y en el costo de seguridad. En la siguiente tabla puede observarse que, así como el capital regulatorio disminuye con una mayor inversión en herramientas de seguridad, así mismo el número de ataques exitosos y el costo de seguridad disminuyen. Este resultado es coherente ya que un menor número de ataques exitosos significa una menor severidad del riesgo operativo y por ende un menor valor en riesgo donde los costos de seguridad tienden a compensar los daños ocasionados por estos ataques.

Tabla 5. Impacto de Inversión en Seguridad en otras variables

INVERSIÓN EN SEGURIDAD	CAPITAL LDA	N° ATAQUES EXITOSOS	COSTO DE SEGURIDAD
$7.000	$583.000	509	$2.602.583
$10.000	$291.000	256	$720.216
$15.000	$134.000	83	$205.203
$55.000	$25,4	0,03	$2.927
$100.000	$2.84 x e-3	3 x e-6	$2.862
$120.000	$5.09 x e-5	6 x e-8	$2.857

3.4 ESCENARIOS ALTERNATIVOS DE INVERSIÓN EN DISUASIÓN

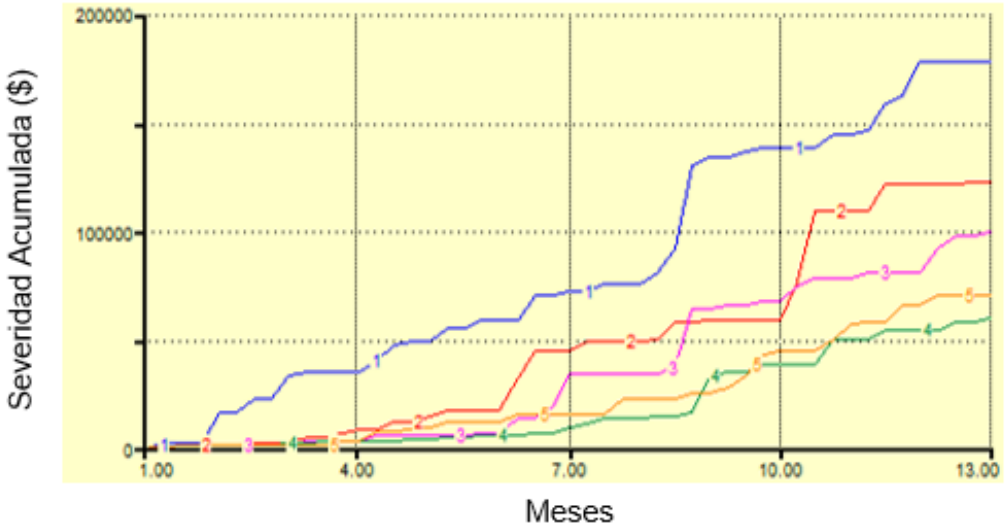
Dado que la inversión en disuasión es una variable de gestión dentro del modelo, es decir, que depende totalmente de la compañía, se realizó un análisis de sensibilidad sobre esta variable con el fin de observar cómo los cambios en la gestión afectan las demás variables relacionadas con el riesgo estudiado, y principalmente el efecto de los diferentes valores de inversión en disuasión en el valor en riesgo operacional.

Partiendo del caso base dónde el valor de inversión en disuasión es de $2000 se decidió realizar el análisis de sensibilidad considerando rangos de variación para la inversión en disuasión. Esto con el fin de identificar en cada uno de los rangos el valor en disuasión que genera el menor valor de capital regulatorio, obteniendo así los valores de inversión en disuasión que generan los menores valores de capital regulatorio.

Para cada uno de los valores de los rangos se simuló el modelo 100 veces, posteriormente a partir del análisis de la gráfica resultante se identificó la inversión dentro del rango que genera los menores impactos, es decir, los menores valores de severidad. Esto debido a que las menores severidades generan a su vez un menor OpVar.

Rango 1: $0 - $4.000

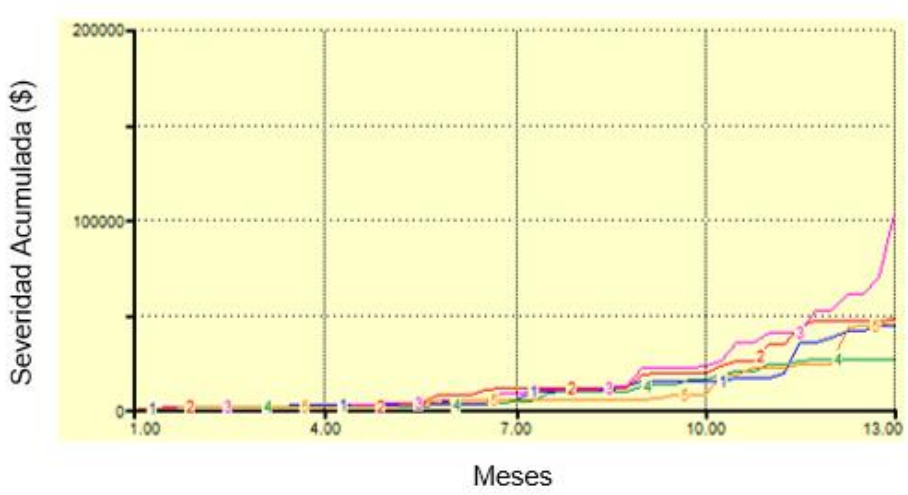
Ilustración 21. Escenario 1 Disuasión



En esta gráfica cada una de las curvas representan en su orden los valores dentro del rango con un incremento de $1.000 en la inversión, así la curva 1 representa una inversión de $0 mientras que la curva 5 representa una inversión de $4000. Puede observarse que la inversión de $3000 es la que genera las menores severidades.

Rango 2: $6.000 - $10.000

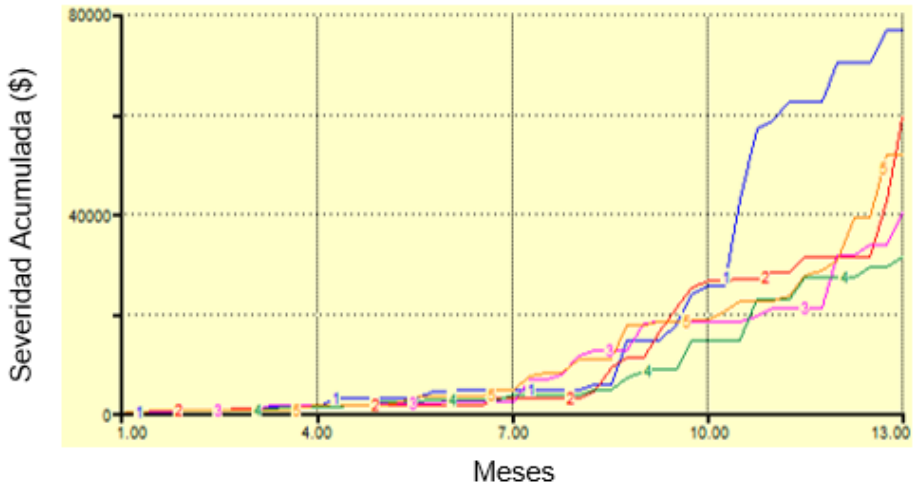
Ilustración 22. Escenario 2 Disuasión



La curva 1 representa una inversión de $6.000 mientras que la curva 5 representa una inversión de $10.000. Puede observarse que la inversión de $9.000 es la que genera las menores severidades, además de que este nivel de inversión genera una severidad menor respecto al valor de $60.000 que ocasiona el nivel óptimo de inversión en disuasión del rango anterior.

Rango 3: $10.000 - $50.000

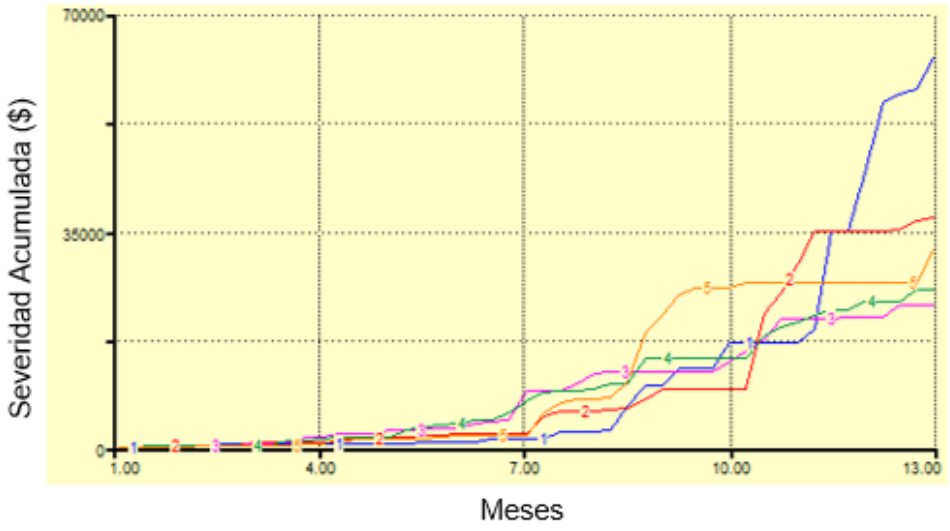
Ilustración 23. Escenario 3 Disuasión



A partir de este rango se optó por incrementar la inversión en disuasión en $10.000 con el fin de determinar hasta qué valor era eficiente para la empresa reducir los niveles de inversión. Así, la curva 1 representa una inversión de $10.000 mientras que la curva 5 representa una inversión de $50.000. Puede observarse que la inversión de $40.000 es la que genera las menores severidades en este rango y respecto a los valores ideales de los rangos anteriores.

Rango 4: $60.000 - $100.000

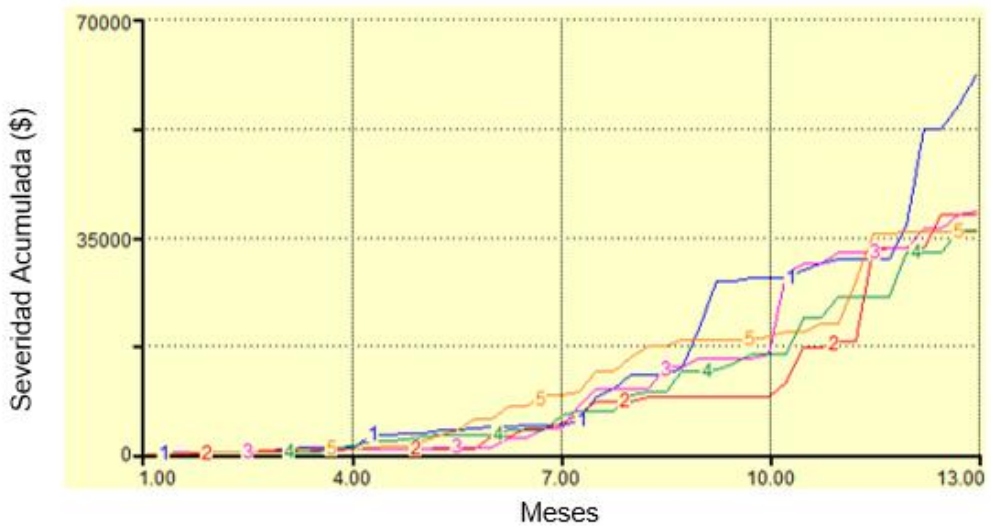
Ilustración 24. Escenario 4 Disuasión



La curva 1 representa una inversión de $60.000 mientras que la curva 5 representa una inversión de $100.000. Puede observarse que la inversión de $80.000 es la que genera las menores severidades en este rango y respecto a los valores ideales de los rangos anteriores.

Rango 5: $100.000 - $140.000

Ilustración 25. Escenario 5 Disuasión

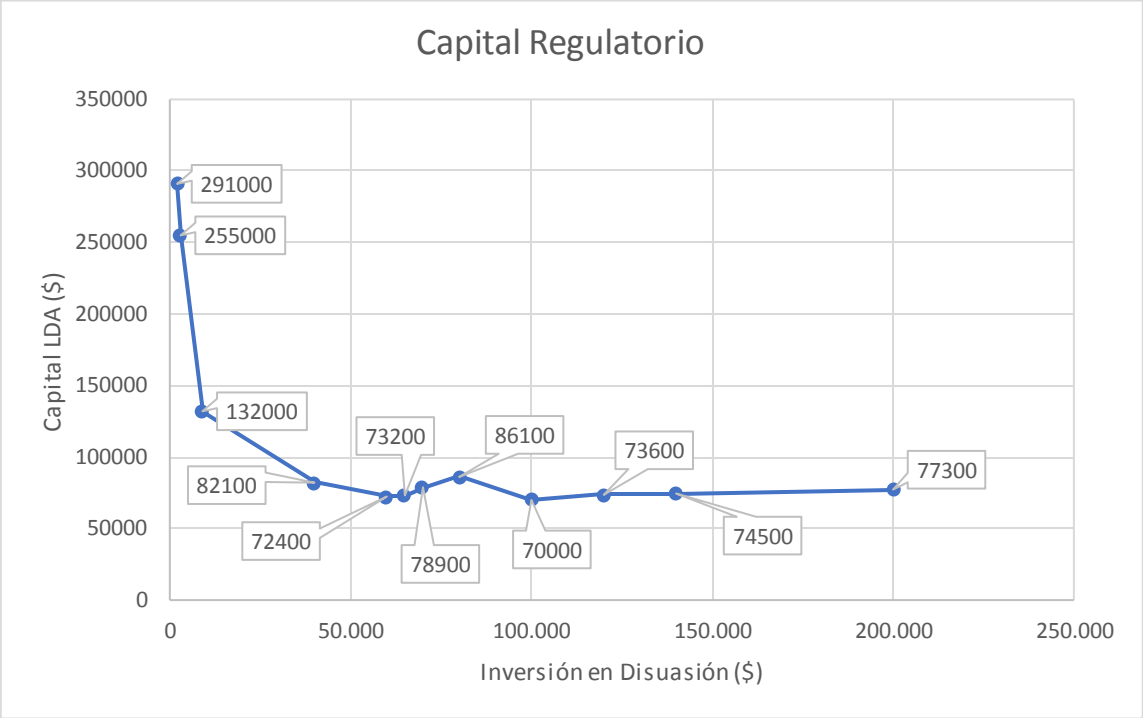


La curva 1 representa una inversión de $100.000 mientras que la curva 5 representa una inversión de $140.000. Puede observarse que la inversión de $140.000 es la que genera las menores severidades

Una vez identificados los valores de inversión en disuasión que generan las menores severidades, se calculó el OpVar para cada uno de estos escenarios. Con el fin de ilustrar que a partir de determinado valor de inversión el OpVar en lugar de disminuir aumenta, se calculó el capital regulatorio para todos los valores del último rango, adicionalmente se calculó el capital para una inversión $200.000. Lo anterior para verificar el comportamiento creciente de la LDA.

El análisis anterior generó como resultado que una inversión de $100.000 en disuasión genera un OpVar de $70.000 siendo este el menor valor de todos los escenarios. En la siguiente gráfica pueden observarse los diferentes OpVar para cada uno de los mejores escenarios de los rangos analizados. La curva de la gráfica demuestra que con una mayor gestión el capital regulatorio de riesgo operativo disminuye. No obstante, este comportamiento decreciente es constante hasta una inversión de $60.000, posterior a este punto, la curva presenta un pico que sugiere que el capital aumenta con una mayor inversión, pero luego vuelve a disminuir con una inversión de $100.000 que es el monto que está generando el menor OpVar. Una inversión más allá de $100.000 parece tener un efecto irrelevante sobre el capital regulatorio.

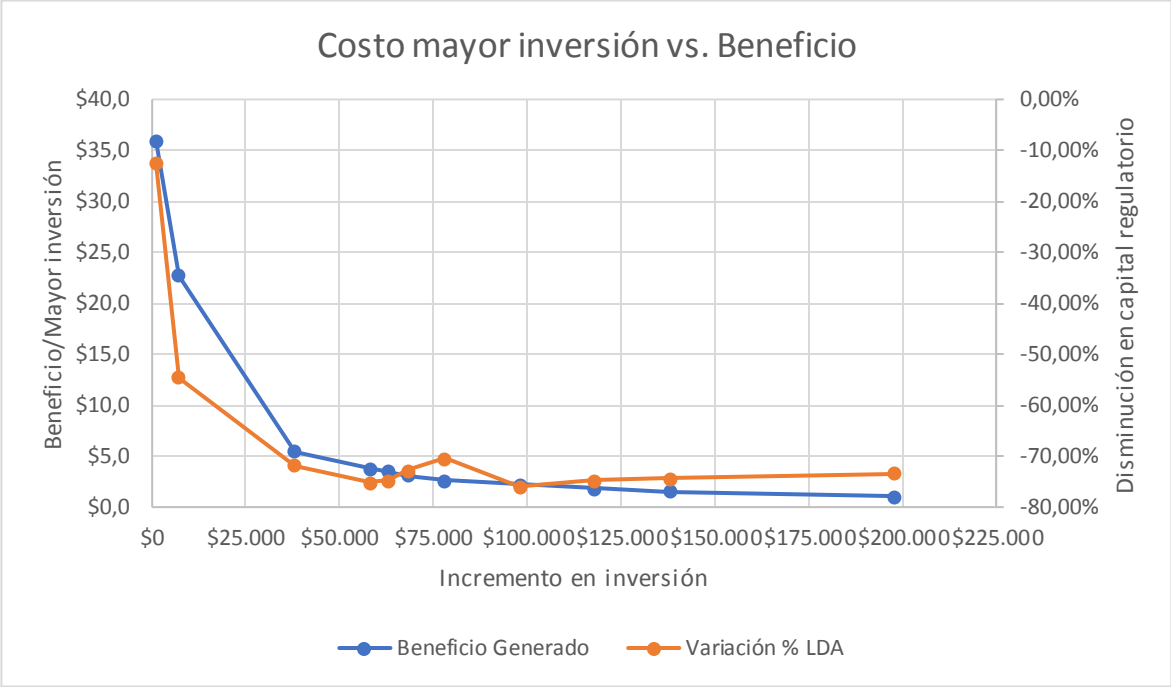
Ilustración 26. Capital Regulatorio vs. Inversión en Disuasión



El comportamiento evidenciado en la anterior gráfica no es concluyente sobre cuál es la inversión en disuasión que generaría mayores beneficios en cuanto a reducción del capital regulatorio, puesto que a simple vista pueden observarse dos mínimos, los cuales serían con una inversión de $60.000 y $100.000. Con el fin de analizar si es conveniente invertir $40.000 de más en disuasión para conseguir una reducción en el OpVaR de tan solo $2400 se realizó un análisis de costo/beneficio, donde el costo corresponde a la inversión adicional que se hace en disuasión y el beneficio a la disminución del capital regulatorio.

Para este análisis se calcularon las variaciones porcentuales del capital regulatorio correspondientes a la inversión adicional necesaria en cada escenario de la gráfica anterior. Además, se halló la proporción costo/beneficio como el beneficio obtenido por la reducción en capital regulatorio dividido la inversión adicional que genera dicho beneficio. En este caso, la inversión adicional se considera como un costo para la empresa puesto que es un desembolso que deberá realizar con el fin de lograr reducir su OpVar. Las relaciones obtenidas se presentan en la siguiente ilustración.

Ilustración 27. Costo Inversión vs. Beneficio



En la Ilustración 27 pueden observarse dos curvas, la curva naranja representa la disminución porcentual del OpVar con los diferentes incrementos de inversión, la curva azul ilustra el beneficio generado por la inversión adicional. Teniendo en cuenta lo anterior, se analizó cuál debería ser la inversión de la empresa si se busca minimizar el costo adicional, maximizando a su vez el beneficio y la variación en el capital LDA.

En conjunto, en la gráfica puede evidenciarse que con una baja inversión adicional se obtiene una mayor proporción de beneficio (curva azul) pero a causa de una menor variación en el OpVar (curva naranja). Al analizar los dos puntos de inversión de interés puede observarse que con una inversión adicional de $58.000 (inversión de $60.000) la empresa obtiene una mayor relación costo beneficio que si invierte $98.000 de más (inversión de $100.000), y que en realidad, la variación porcentual del capital regulatorio respecto al monto inicial difiere en tan solo 0.83%. Por tanto, puede concluirse que si bien con un monto de inversión de $100.000, se obtiene el menor OpVar, ésta no sería una inversión óptima puesto que su beneficio respecto a la inversión realizada es menor que si se invierte $60.000. En la primera se obtiene un beneficio de $2.3 por cada dólar adicional invertido, mientras que en la segunda se obtiene un beneficio de $3.8.

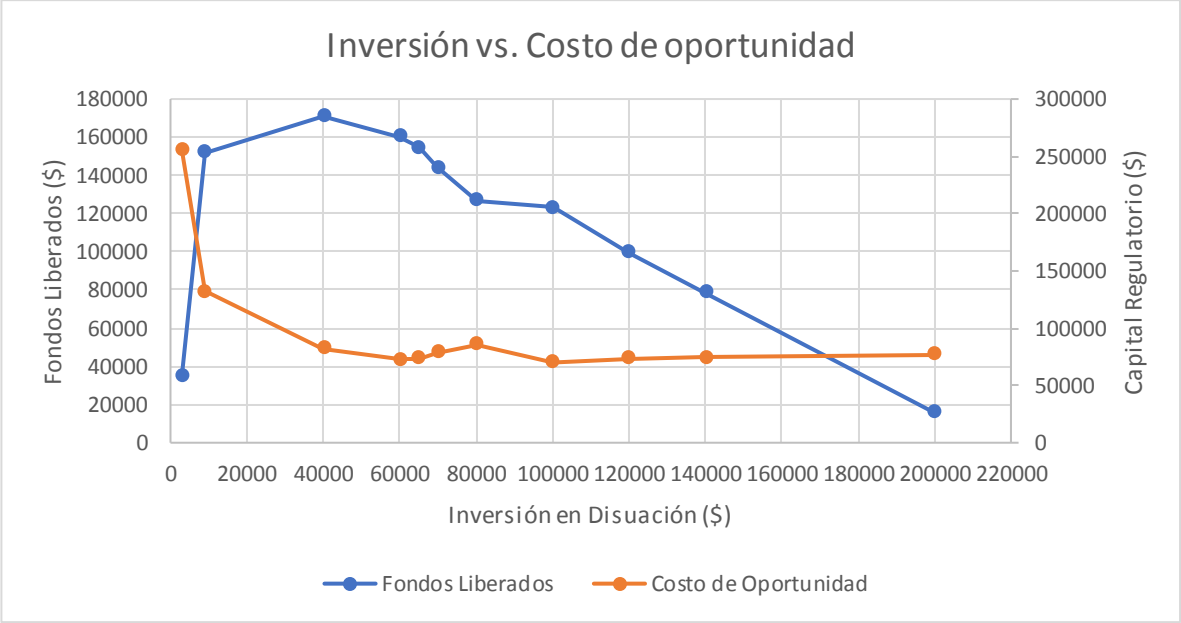
No obstante, la gráfica anterior también puede entenderse como un marco de decisión para las empresas, donde dependiendo de la situación financiera o de los intereses de inversión de la misma, se puede analizar cuál sería la inversión adicional más conveniente

dependiendo si el interés es lograr un mayor costo-beneficio en la inversión o si este consiste en disminuir en la mayor proporción posible el capital regulatorio que deben prever para el cubrimiento de los eventos de riesgo operativo.

Como se expresó anteriormente, normalmente las empresas calculan el OpVar para conocer cuánto capital deben tener en reserva para cubrir los eventos de riesgo que se presenten durante un año. Sin embargo, dicho capital regulatorio en reserva puede interpretarse como un costo de oportunidad para las entidades puesto que es un capital que de alguna forma se está dejando de invertir en otras actividades rentables. Por tanto, la disminución del OpVar significa también disminuir el costo de oportunidad de la empresa al liberar fondos retenidos.

La Ilustración 28 muestra a su vez el costo de oportunidad correspondiente a la disminución en el capital regulatorio en cada escenario de inversión, y la cantidad neta de fondos liberados. La cantidad neta de fondos liberados es la disminución del OpVar respecto al escenario base menos la inversión necesaria adicional (costo). Así, puede observarse como a medida que el costo de oportunidad es más pequeño, la liberación de fondos también lo es, lo que lleva igualmente a concluir que a partir de cierto punto donde no se obtienen mayores variaciones en el OpVar, tener una inversión adicional no es rentable puesto que la relación costo-beneficio es baja, y además no genera una liberación de fondos significativa que pueda utilizarse en otras actividades rentables.

Ilustración 28. Inversión vs. Costo de oportunidad



Finalmente se analizó el impacto de la inversión en disuasión en el número de ataques exitosos y en el costo de seguridad. En la siguiente tabla puede observarse que, así como

el capital regulatorio disminuye con una mayor inversión en disuasión, así mismo el número de ataques exitosos y el costo de seguridad disminuyen. Este resultado es coherente ya que un menor número de ataques exitosos significa una menor severidad del riesgo operativo y por ende un menor valor en riesgo.

Igualmente, se confirma lo analizado anteriormente sobre una inversión superior a $60.000 ya que puede verse que una mayor inversión tiene impacto negativo en el número de ataques exitosos, por ende, la severidad no disminuye, pero el costo de seguridad sí aumenta. En el caso de una inversión de $100.000 el costo de seguridad disminuye pero el número de ataques exitosos aumenta respecto a una inversión de $60.000, además previamente se concluyó que esta inversión no sería rentable para la empresa por la relación costo-beneficio.

Tabla 6. Impacto de Inversión en Disuasión en otras variables

INVERSIÓN EN DISUASIÓN	CAPITAL LDA	N° ATAQUES EXITOSOS	COSTO DE SEGURIDAD
$2.000	$291.000	256	$720.216
$9.000	$132.000	121	$267.304
$40.000	$82.100	61	$119.856
$60.000	$72.400	16	$115.429
$100.000	$70.000	58	$69.205
$140.000	$74.500	68	$141.739
$200.000	$77.300	72	$189.007

3.5 ESCENARIO COMPARATIVO DE INVERSIONES

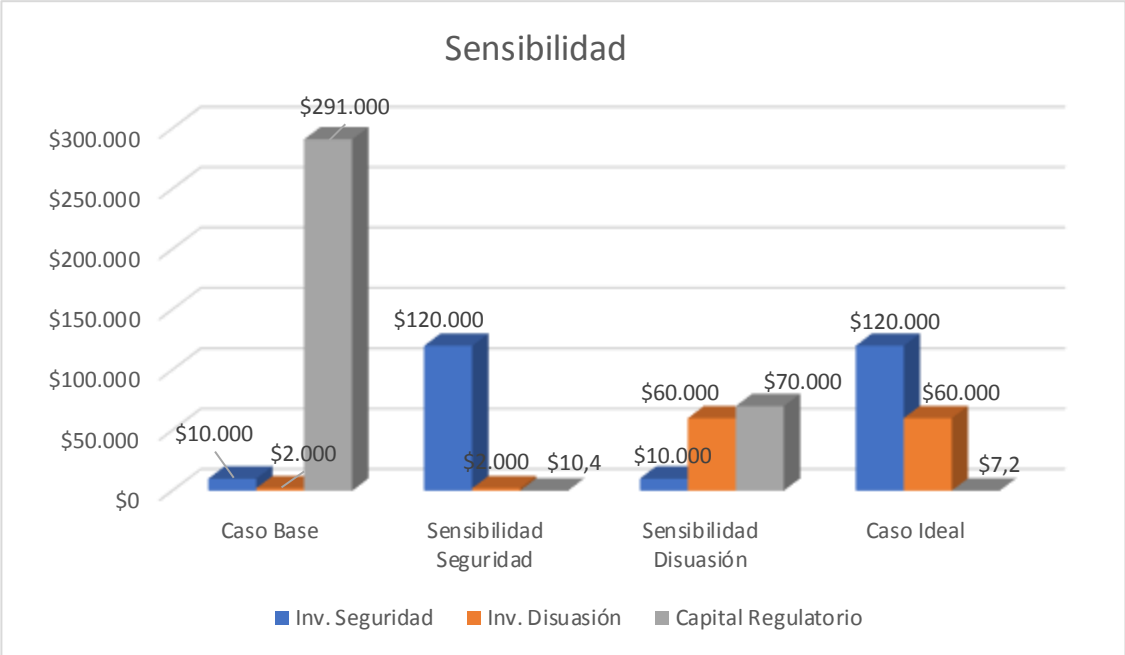
Con el fin de determinar cuál de las dos variables analizadas (inversión en seguridad o inversión en disuasión) influye más sobre el capital regulatorio, se hizo una comparación entre los valores invertidos en ambas variables y sus resultados respectivos en cuanto a severidad y capital LDA (ver Tabla 7). En este sentido, se puede observar que la inversión en seguridad es la variable que más influye sobre el capital regulatorio, por lo cual esta inversión es la que más se puede gestionar desde la empresa para tener un control sobre el dinero que se debe tener en reserva para soportar los eventos de riesgo que se pueda presentar.

Lo anterior se puede confirmar con la Ilustración 29, pues en esta se evidencia que el menor valor de capital regulatorio se obtiene si la empresa decide invertir $120.000 en seguridad (mejor escenario) y $60.000 en disuasión (mejor escenario), caso ideal para la empresa de estudio.

Tabla 7. Inversión en Seguridad vs. Inversión en Disuasión

INVERSIÓN EN SEGURIDAD	SEVERIDAD ACUMULADA	CAPITAL LDA	INVERSIÓN EN DISUASIÓN	SEVERIDAD ACUMULADA	CAPITAL LDA
$7.000	$254.255	$583.000	$2.000	$128.796	$291.000
$10.000	$128.796	$291.000	$9.000	$57.200	$132.000
$15.000	$41.375	$134.000	$40.000	$37.000	$82.100
$55.000	$13,6	$24.5	**$60.000**	**$32.800**	**$72.400**
$100.000	$2 x e-3	$2.84 X E-3	$100.000	$34.200	$70.000
$120.000	**$3 x e-5**	**$5.1 X E-5**	$140.000	$34.700	$74.500

Ilustración 29. Caso Ideal Sensibilidad



4. CONCLUSIONES Y CONSIDERACIONES FINALES

El presente estudio propone un modelo de gestión del riesgo operativo para entidades financieras basado en la dinámica de sistemas con el propósito de generar una solución más robusta a las existentes en la actualidad frente al riesgo operativo. En general los métodos de gestión del riesgo operativo se centran únicamente en la cuantificación del riesgo, es decir, en el cálculo del OpVar como el capital regulatorio que las entidades financieras deben poseer para responder frente a los diferentes eventos de riesgo operativo. No obstante, estos enfoques no toman en cuenta las interrelaciones existentes entre las variables que intervienen en los eventos de riesgo, y por tanto, la gestión del riesgo se convierte en un asunto más empírico que estructurado.

De esta forma, se desarrolló un modelo de dinámica de sistemas para el riesgo operativo de seguridad de los sistemas basado en el modelo dinámico propuesto por Derek L. Nazareth y Jae Choi (2014), los cuales a su vez se basaron en un modelo previo adicionando variables de gestión y ajustando las ecuaciones que determinan las construcciones del modelo. El principal aporte de este estudio es la incorporación de variables en el modelo dinámico para capturar las frecuencias y severidades del evento de riesgo producto de las interacciones dinámicas entre las variables que intervienen en dicho riesgo. Es así como esta aproximación permite no solo gestionar las variables que intervienen en la frecuencia del evento de riesgo, sino también la cuantificación del riesgo por medio de la distribución agregada de pérdidas, obteniendo así el OpVar para distintos niveles de gestión.

Un hallazgo importante de este estudio es que la gestión activa de las entidades tiene un impacto positivo en el monto de capital regulatorio que éstas deben retener para hacer frente a sus eventos de riesgo operativo. La gestión activa en el contexto del estudio puede entenderse como la manipulación de las variables cuyo valor o comportamiento dependen exclusivamente de la compañía, como es el caso de la inversión en herramientas de seguridad e inversión en disuasión. En la implementación de la metodología planteada pudo observarse que un aumento de la inversión generó menores valores de capital regulatorio, lo que en la práctica también se traduce en un menor costo de oportunidad para las entidades, puesto que esa reducción en capital regulatorio puede ser invertido en alguna opción rentable en lugar de estar retenido para contingencias.

A partir del análisis de sensibilidad realizado al modelo, se pudo determinar que, de las dos variables de gestión del modelo, la inversión en herramientas de seguridad es aquella que genera un mayor impacto sobre la severidad acumulada, y por ende sobre el capital regulatorio a lo largo del tiempo. Así, si la empresa realiza una correcta gestión de esta inversión, dejando las demás variables constantes, tendrá que destinar menor cantidad de dinero para soportar el riesgo operacional, y así podrá realizar mayor cantidad de actividades de inversión que beneficiará el crecimiento de la misma. Igualmente, si la empresa tiene la capacidad económica suficiente, se recomienda realizar las inversiones óptimas tanto en disuasión como en herramientas de seguridad, esto con el fin de obtener el mínimo valor posible para el capital regulatorio.

Otra ventaja que tiene el modelo propuesto frente a los demás modelos existentes para la gestión del riesgo operativo es que, este al ser dinámico permite modificar los parámetros que determinan las construcciones del modelo sin alterar la estructura causal, lo cual es eficiente al momento de evaluar los efectos que diferentes variables pueden tener en el monto total de capital regulatorio operativo. Por otra parte, el modelo propuesto es flexible para ser adaptado a los demás tipos de riesgo operativo y a cualquier tipo de entidad financiera, teniendo en cuento que lo más importante es la delimitación del modelo, es decir en las variables que intervienen en el riesgo específico y las interacciones entre ellas.

En cuanto a la elaboración de futuros trabajos se recomienda seguir estudiando el riesgo operacional y otros tipos de riesgo que sufren las empresas en su operación del día a día, no solo desde las estructuras que soportan los patrones, sino también desde los modelos mentales que están detrás de las estructuras, esto con el fin de entender más a fondo cómo las mismas empresas pueden contribuir a la disminución del capital regulatorio desde su gestión.

Por otra parte, para el planteamiento de futuros modelos se recomienda utilizar una distribución mixta entre la distribución Lognormal y la distribución Generalizada de Pareto (GPD) para ajustar los datos de severidad del modelo, esto con el fin de evitar sub-valoraciones del OpVar. De igual forma, para el momento de realizar las simulaciones del mismo, se recomienda utilizar el muestreo hipercubo latino ya que este requiere de menos cantidad de iteraciones para cubrir todo el rango de la distribución, y por ende brindar una mayor precisión en el cálculo del OpVar.

En conclusión, se considera que la aproximación aquí propuesta puede ser incluida por las entidades financieras dentro de sus modelos de gestión de riesgo operativo, puesto que al abarcar tanto el nivel de eventos, patrones y estructuras otorga a la entidad una mayor comprensión del funcionamiento del riesgo, y por tanto un mayor espectro de acción para la gestión y disminución del impacto del mismo.

REFERENCIAS

Aguirre Botero, Y. C., & Mesa Callejas, R. J. (14 de diciembre de 2009). Lecciones de la crisis financiera internacional:. *Semestre económico, 12*(25), 61-79.

Arbelaez, J. C., Franco, L. C., Betancur, C., Murillo, J. G., Gallego, P. A., Henao, V. M., . . . Salazar, L. F. (28 de Agosto de 2006). Riesgo Operacional: Reto Actual de las Entidades Financieras. *Revista Ingernierias Universidad de Medellín*, 14. Recuperado el 04 de 09 de 2017

Banco de España. (s.f.). *BCBS.* Recuperado el 04 de Septiembre de 2017, de https://www.bde.es/bde/es/areas/supervision/actividad/BCBS/BCBS.html

Banco de la República. (2013). El sistema financiero colombiano: estructura y evolución reciente. *Revista del Banco de la República, 1023*, 17. Recuperado el 04 de 09 de 2017

Bank, Austrian National. (1999). *Guidelines on Market Risk.* Recuperado el 18 de Agosto de 2017

Basel Committee on Banking Supervision. (2016). *StandardisedMeasurement approach for operational risk.* Bank for Internatioanl Settlements.

Basle Committee on Banking Supervision. (Octubre de 2002). *The Bank for International Settlements (BIS).* Recuperado el 19 de Agosto de 2017, de Quantitative Impact, Technical Guidance,: http://www.bis.org.

Brechmann, E., Czado, C., & Paterlini, S. (2013). *Flexible dependence modeling of operational risk losses and its impact on total capital requirements.* Garching-Hochbrück: Elsevier.

BVSDE:Colombia. (2010). Recuperado el 25 de julio de 2017, de http://www.bvsde.paho.org/bvsacd/eco/020425/020425-04.pdf

Chaudhuri, A., & Ghosh, S. K. (2016). *Quantitative Modeling of Operational Risk in Finance and Banking Using Possibility Theory* (Vol. 331). Londres: Springer.

Clemente, A. R. (24 de febrero de 2010). *Organizaciones Inteligentes*. Obtenido de https://www.xing.com/communities/posts/holismo-1005216612

Coll, J. C. (octubre de 2007). KENNETH E. BOULDING, ECONOMISTA Y PACIFISTA. *Textos de economía paz y seguridad, 1*(1). Obtenido de http://www.eumed.net/rev/tepys/01/jcmc-1.htm

Coltefinanciera. (20 de agosto de 2017). *¿Cómo está estructurado el Sistema Financiero en Colombia?* Recuperado el 04 de 09 de 2017, de

http://www.coltefinanciera.com.co/educacion-financiera/sistema-financiero/385-como-esta-estructurado-el-sistema-financiero-en-colombia

Comité de Supervisión Bancaria de Basilea. (2003). *Buenas prácticas para la gestión y supervisión del riesgo operativo.* Secretaría del Comité de Supervisión Bancaria de Basilea . Recuperado el 8 de agosto de 2017, de http://www.bis.org/publ/bcbs96esp.pdf

Comité de Supervisión Bancaria de Basilea. (2013). *Carta estatutaria.* Bank for International Settlements. Recuperado el 04 de 09 de 2017

Compañía Aseguradora de Finanzas S.A. (2011). *Cartilla de Riesgo Operativo.*

de Fontnouvelle, P., De Jesus-Rueff, V., Jordan, J., & Rosengren, E. (2003). *Using Loss Data to Quantify Operational Risk.* Boston.

Di Pietro, F., Irimia-Diéguez, A. I., & Oliver-Alfonso, M. D. (2012). Cuestiones abiertas en la modelización del riesgo operacional en los acuerdos de Basilea: el umbral de pérdidas y la distribución de severidad. *UNIVERSIA Business Review.*

Eckert, C., & Gatzert, N. (2016). *Modeling operational risk incorporating reputation risk: An integrated analysis for financial firms.* Nürnberg: Elsevier. Recuperado el 20 de Julio de 2017

Estaire, F. S. (2012). *Psicólogos en Madrid EU*. Obtenido de Teoría General de Sistema de von Bertalanffy: http://psicologosenmadrid.eu/teoria-general-de-sistemas-de-von-bertalanffy/

FAO. (s.f.). *DEPÓSITO DE DOCUMENTOS DE LA FAO*. Obtenido de CAPÍTULO 3: DEFINICIÓN DE UN SISTEMA: http://www.fao.org/docrep/004/W7451S/W7451S03.htm

Federal Reserve Bankof Boston. (2014). *Internal Measurement Approach (Foundation Model).*

Franco Arbelaéz, L. C., & Murillo Gómez, J. G. (2008). Loss Distribution Approach (LDA): Metodología Actuarial Aplicada al Riesgo Operacional. *Revista Ingenierías Universidad de Medellín*, 143-156.

Galloppo, G., & Rogora, A. (2011). What has worked in operational risk? *Global Journal of Business Research, 53*. Recuperado el 7 de agosto de 2017

Giudici, P. (2007). *Scorecard Models for Operational Risk Management.* Pavia.

Goodman, M. (2002). *The iceberg Model.* Hopkinton, MA: Innovation Associates Organization Learning.

Guertler, B., & Spinler, S. (2015). *When does operational risk cause supply chain enterprises to tip? A simulation of intra-organizational dynamics.* Elsevier. Recuperado el 20 de Julio de 2017

Guijarro, J. C. (2013). *eumed.net*. Obtenido de MODELOS DE ENFOQUE DE MEDICIÓN AVANZADO DEL RIESGO OPERATIVO (EMA): http://www.eumed.net/ce/2011a/jcg.htm

Hernández Correa, G. (2016). *Avances en la supervisión y regulación del Sistema Financiero Colombiano.* Superintendencia Financiera de Colombia, Bogotá. Recuperado el 1 de agosto de 2017

Heylighen, F. (diciembre de 1991). *Principia Cybernetica and Principia Mathematica*. Obtenido de http://pespmc1.vub.ac.be/PRMAT.html

Heylighen, F. (14 de enero de 2000). *Referencing pages in Principia Cybernetica Web*. Obtenido de http://pespmc1.vub.ac.be/REFERPCP.html

Heylighen, F., & Joslyn, C. (noviembre de 1992). *Principia Cybernetica Web*. Obtenido de http://pespmc1.vub.ac.be/SYSTHEOR.html

Heylighen, F., & Joslyn, C. (agosto de 1993). *Principia Cynernetica Web*. Obtenido de http://pespmc1.vub.ac.be/CRITIC.html

Huigens, A. (2005). *Systems Thinking, the iceberg theory of Daniel Kim.* FURMAN Center for Corporate and Professional Development. Recuperado el 12 de agosto de 2017, de http://www.fusbp.com/wp-content/uploads/2010/07/systems_thinking-explained.pdf

Iman, R., Davenport, J., & Zeigler, D. (1980). *Latin Hypercube Sampling.* Albuquerque: Sandia Laboratories.

Jiménez Rodríguez, E. J., & Matín Marín, J. L. (2005). El nuevo acuerdo de Basilea y la gestión delriesgo operacional. *UNIVERSIA BUSINESS REVIEW*, 6. Obtenido de http://www.redalyc.org/html/433/43300704/

Kessler, A. M. (2002). *Value at Risk (VaR) – Usability and Reliability in the Short and Long Run.* Universidad de Estocolmo, Estocolmo. Recuperado el 18 de Agosto de 2017

Kessler, A. M. (2007). *A Sytemic Approach Framework for Operational Risk.* Tesis doctoral , Stockholm University, Kista. Recuperado el 19 de agosto de 2017

Kim, D. H. (1996). From Event Thinking to Systems Thinking. *The Systems Thinker, 7*(4), 6-7.

KUBERNÉTICA. (s.f.). La cibernética de Norbert Wiener. *KUBERNÉTICA*. Obtenido de http://www.santiagokoval.com/2017/01/09/la-cibernetica-de-norbert-wiener/

Law, A. (2007). *Simulation Modeling and Analysis.*

Li, J., Yi, S., Feng, J., & Shi, Y. (2011). *Modelling the mitigation impact of insurance in Operational Risk management.* Beijing: Elsevier.

López Pacheco, D. (2009). *Riesgo Operacional: Conceptos y Mediciones.* Dirección de Estudios y Análisis Financiero. Recuperado el 7 de agosto de 2017

Management Solutions. (2012). *Convención Impactos de BIS III en la región.*

Management Solutions. (2012). *Convención Impactos del BIS III en la región.* Recuperado el 04 de Septiembre de 2017

Moosa, I. A. (2007). Operational Risk: A Survey. *Institutions & Instruments, 16*(4).

Mora Valencia, A. (2010). *Cuantificación del Riesgo Operativo en Entidades Financieras en Colombia.* Bogotá.

Mora, A. (2008). Una recomendación para cuantificar el riesgo operativo en entidades. *Colegio de Estudios Superiores de Administración - CESA.*

Mora, A. (2009). *Una recomendación para cuantificar el riesgo operativo en entidades financieras de Colombia.* Bogotá.

Nazareth, D. L., & Choi, J. (2014). *A system dynamics model for information security management.* Milwaukee.

Nieto Giménez, M. Á., & Gómez Fernández, I. (2006). *RIESGO OPERACIONAL Aspectos relevantes de los métodos: Aspectos relevantes de los métodos de indicador básico y estándar .* Madrid.

O'Brien, N., Smith, B., & Allen, M. (Julio de 1999). The case for quantification - Operational Risk Supplement. *Risk Magazine*. Recuperado el 19 de Agosto de 2017

Otero, P., & Venerio, O. (2009). *Determinación del requerimiento de capital por riesgo operacional.*

Pakhchanyan, S. (2016). Operational Risk Managemet in Financial Institutions: A Literature Review. *International Journal of Financial Studies*.

Peña, A., Bonet, I., & Lochmuller, C. (2018). Flexible inverse adaptive fuzzy inference model to identify the evolution of Operational Value at Risk for improving operational risk management. *Applied Soft Computing*.

Risk Concepts. (Enero de 2003). *Risk Management and Insurance Services from Risk Concepts.* Recuperado el 18 de Agosto de 2017, de http://www.riskconcepts.com/EnterpriseRiskManagementServices.htm

Romero, L. R. (2009). *Riesgo operacional: Implementación del Método Estándar y Estándar Alterativo en Basilea II.*

Santini, F., Kokash, N., & Arbab, F. (2012). *Modeling and Simulation of Selected operational IT Risk in the Banking Sector.* Holanda.

Shah, S. (2001). *Operational Risk Management-Casualty Actuarial Society 2001 Seminar on Understanding the Enterprise Risk Management Process.* San Francisco: Towers Perrin.

Sterman, J. D. (2002). *System Dinamics: Systems Thinking and Modeling for a Complex World.* Cambridge.

Superintendencia de Bancos e Instituciones Financieras Chile. (2009). *Riesgo Operacional - Conceptos y Mediciones.*

Superintendencia Financiera de Colombia. (2006). *Circular Externa 049 de 2006.*

Superintendencia Financiera de Colombia. (2007). *Circular Externa 041 de 2007.* CAPITULO XXIII: Reglas relativas a la administración del riesgo operativo. Recuperado el 10 de agosto de 2017

Williams, B., & Hummelbrunner, R. (2011). Systems Concepts in Action . En B. Williams, & R. Hummelbrunner. Stanford.

ANEXO 1. ECUACIONES MODELO

1. STOCKS

- $Costo\ Seguridad\ Acumulado = 0$
- $Inversión\ de\ Disuasión\ Acumulada = 100.000$
- $Reportes\ Acumulados = 1$
- $Inversión\ en\ Herramientas\ de\ Seguridad\ Acumulada = 55.000$
- $Vulnerabilidad\ Acumulada = 0$
- $Daño = 0$
- $Total\ Ataques\ Prevenidos = 0$
- $Severidad\ Acumulada = 0$
- $Ataques\ Exitosos\ Acumulados = 0$

2. ENTRADAS

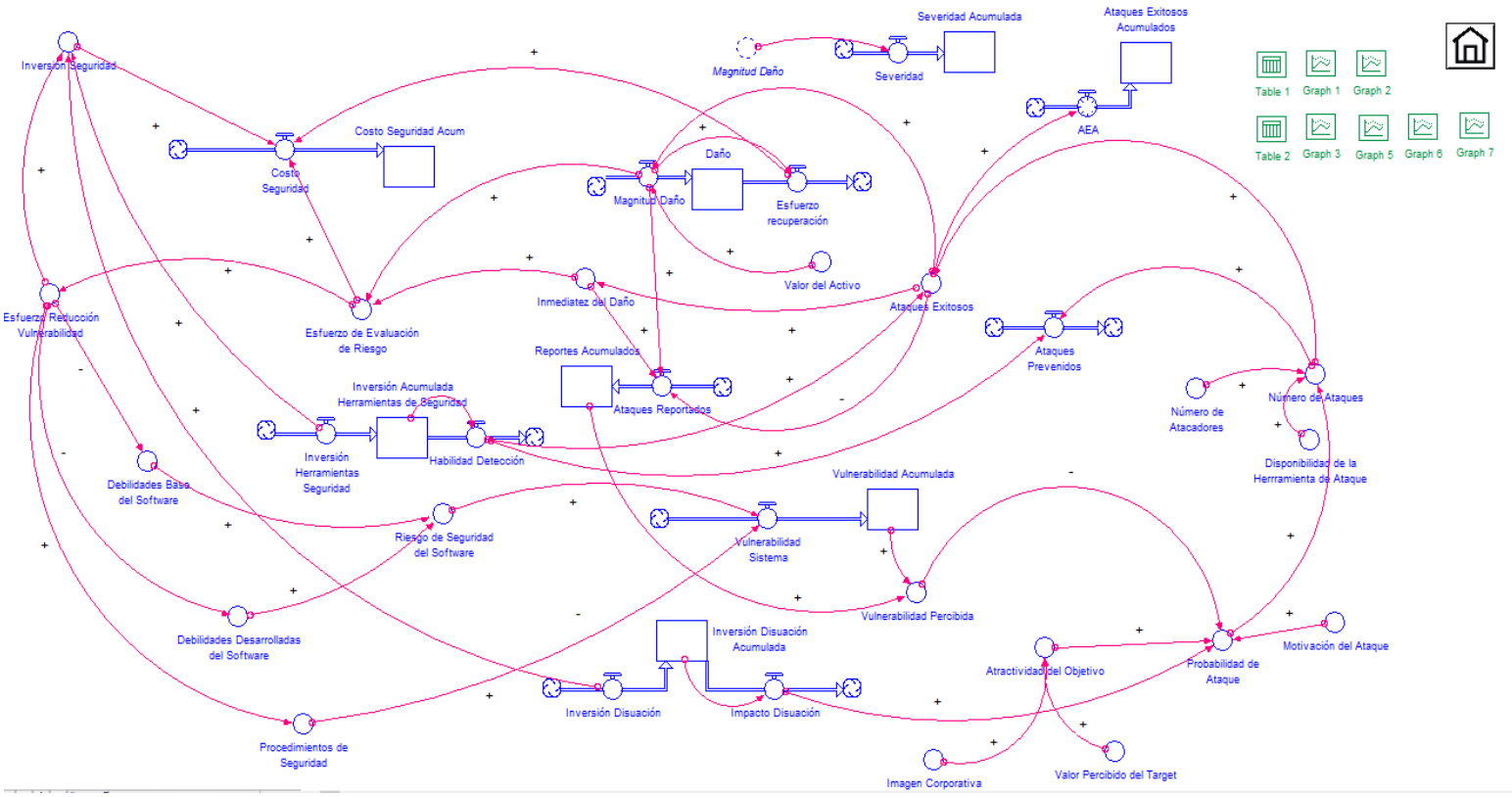
- $Valor\ del\ Activo = 5.000.000$
- $Motivación\ del\ Ataque = 0.5$
- $Disponibilidad\ de\ la\ Herramienta\ de\ Ataque = 0.5$
- $Inversión\ en\ Disuasión = 2.000 * PULSE(0.25,6,6)$
- $Número\ de\ Atacadores = 100$
- $Imagen\ Corporativa = 0.5$
- $Valor\ Percibido\ del\ Target = 0.5$
- $Inversión\ en\ Herramientas\ de\ Seguridad = 5.000 * PULSE\ (0.25,0,12)$

3. VARIABLES

- $Debilidades\ Base\ del\ Software = 0.75 * EXP(-0.01 * Esfuerzo\ Reducción\ de\ Vulnerabilidad)$
- $Debilidades\ Desarrolladas\ del\ Software = 0.5 * EXP(-0.01 * Esfuerzo\ Reducción\ de\ Vulnerabilidad)$
- $Inmediatez\ del\ daño = 1 - EXP(-0.2 * \frac{Ataques\ Exitosos}{10})$
- $Magnitud\ del\ Daño = IF[RANDOM(0,1) > 0.5]\ THEN[0.0002 * Valor\ del\ Activo * Ataques\ Exitosos * EXPRANDOM(1)]\ ELSE(0)$
- $Habilidad\ de\ Detección = 1 - EXP(-0.001 * \frac{Inversión\ en\ Herramientas\ de\ Seguridad\ Acumulada}{5})$
- $Impacto\ de\ Disuasión = 1 - EXP(-0.125 * \frac{Inversión\ de\ DisuasiónAcumulada}{1000})$
- $Número\ de\ Ataques = RANDOM[\{2.5 * (Probabilidad\ de\ Ataque * Número\ de\ Atacadores) * (Disponibilidad\ de\ la\ Herramienta\ de\ Ataque^{1.1})\},\{7.5 * (Probabilidad\ de\ Ataque * Número\ de\ Atacadores) * (Disponibilidad\ de\ la\ Herramienta\ de\ Ataque^{1.1})\},0]$

- $Vulnerabilidad\ Percibida = IF(0.01 * Vulnerabilidad\ Acumulada * Reportes\ Acumulados < 1)\ THEN(0.01 * Reportes\ Acumulados * Vulnerabilidad\ Acumulada)\ ELSE(1)$
- $Ataques\ Prevenidos = Habilidad\ de\ Detección * Número\ de\ Ataques$
- $Probabilidad\ de\ Ataque = IF\left[\frac{\left\{3.6*\left(0.1+\frac{Vulnerabilidad\ Percibida-0.1}{Vulnerabildiad\ Percibida+1}\right)*\left(0.3+\frac{Atractividad\ del\ Objetivo-0.1}{Atractividad\ del\ Objetivo+0.5}\right)*\left(0.1+\frac{Motivación\ del\ Ataque-0.1}{Motivación\ del\ Ataque+1}\right)\right\}}{Impacto\ de\ Disuasión} < 1\right] THEN\left[\frac{\left\{3.6*\left(0.1+\frac{Vulnerabilidad\ Percibida-0.1}{Vulnerabildiad\ Percibida+1}\right)*\left(0.3+\frac{Atractividad\ del\ Objetivo-0.1}{Atractividad\ del\ Objetivo+0.5}\right)*\left(0.1+\frac{Motivación\ del\ Ataque-0.1}{Motivación\ del\ Ataque+1}\right)\right\}}{Impacto\ de\ Disuasión}\right] ELSE(1)$
- $Esfuerzo\ de\ Recuperación = RANDOM(Magnitud\ del\ Daño * 0.5, Magnitud\ del\ Daño * 1.5, 0)$
- $Ataques\ Reportados = IF(Ataques\ Exitosos * Magnitud\ del\ Daño * Inmediatez\ del\ Daño = 0)\ THEN(1)\ ELSE\left[LOG(Ataques\ Exitosos) * \frac{Magnitud\ del\ Daño^{Inmediatez\ del\ Daño}}{10}\right]$
- $Esfuerzo\ de\ Evaluación\ de\ Riesgo = Magnitud\ del\ Daño^{Inmediatez\ del\ Daño}$
- $Costo\ de\ Seguridad = Inversión\ en\ Seguridad + (Esfuerzo\ de\ Recuperación * 5) + (Esfuerzo\ de\ Evaluación\ de\ Riesgo * 50)$
- $Inversión\ en\ Seguridad = (Esfuerzo\ Reducción\ de\ Vulnerabilidad * 50) + Inversión\ en\ Disuasión + Inversión\ en\ Herramientas\ de\ Seguridad$
- $Procedimientos\ de\ Seguridad = 1 - EXP(-0.5 * \frac{Esfuerzo\ Reducción\ de\ Vulnerabilidad}{100})$
- $Riesgo\ de\ Seguridad\ Software = 2.7 * \left[\frac{Debilidades\ Desarrolladas\ del\ Software}{Debilidades\ Desarrolladas\ del\ Software+1}\right] * \left[\frac{Debilidades\ Base\ del\ Software}{Debilidades\ Base\ del\ Software+0.5}\right]$
- $Ataques\ Exitosos = (1 - Habilidad\ de\ Detección) * Número\ de\ Ataques$
- $Vulnerabilidad\ del\ Sistema = Riesgo\ de\ Seguridad\ del\ Software * EXP(-2 * Procedimientos\ de\ Seguridad$
- $Atractividad\ del\ Objetivo = 2.5 * \left[\frac{Imagen\ Corporativa}{Imagen\ Corporativa+1}\right] * \left[\frac{Valor\ Percibido\ del\ Target+0.2}{Valor\ Percibido\ del\ Target+0.5}\right]$
- $Esfurzo\ Reducción\ de\ Vulnerabilidad = RANDOM[(Esfuerzo\ de\ Evaluación\ de\ Riesgo * 0.5), (Esfuerzo\ de\ Evaluación\ de\ Riesgo * 1.5), 0]$

ANEXO 2. DIAGRAMA DE FLUJOS Y NIVELES



Fuente: elaboración propia